KASPERSKY LAB

Kaspersky Anti-Virus® Personal 5.0

USER'S GUIDE

KASPERSKY ANTI-VIRUS® PERSONAL 5.0

User's Guide

© Kaspersky Lab
http://www.kaspersky.com

Revision date: January, 2006

Contents

CHAPTER 1. INTRODUCTION 6
1.1. Computer viruses and malicious computer programs 6
1.2. The purpose and major functions of Kaspersky Anti-Virus® Personal 8
1.3. What's new in Version 5.0? 10
1.4. Hardware and software system requirements 12
1.5. Distribution Kit 12
1.6. Services provided for registered users 13

CHAPTER 2. INSTALLING THE APPLICATION ON YOUR COMPUTER 14

CHAPTER 3. IF YOUR COMPUTER IS INFECTED… 21
3.1. Signs of infection 21
3.2. What should you do if you notice symptoms of infection 22

CHAPTER 4. ANTI-VIRUS PROTECTION USING KASPERSKY ANTI-VIRUS DEFAULT SETTINGS 24
4.1. Real-Time Protection 24
4.2. On-Demand Scan 25
4.3. Updating the anti-virus database 26

CHAPTER 5. APPLICATION INTERFACE 28
5.1. System tray icon 28
5.2. Shortcut menu 29
5.3. Main application window: general layout 30
5.3.1 Protection tab 32
5.3.2 Settings tab 33
5.3.3 Support tab 34
5.4. Scan window 35
5.5. Application reference system 36

CHAPTER 6. PREVENTING VIRUS INFECTIONS 37
6.1. When do I need to perform an anti-virus scan? 38
6.2. Scan settings to be used 39

6.3. Starting an on-demand scan 44
6.4. Scheduled full scan 45
6.5. On-demand scan of selected objects 46
6.6. Scanning archives 49

CHAPTER 7. SCANNING A REMOVABLE DRIVE 51

CHAPTER 8. CONFIGURING REAL-TIME PROTECTION 53
8.1. Checking the protection status 53
8.2. Specifying application actions and setting the protection level 53
8.3. Stopping real-time protection 57

CHAPTER 9. PROTECTING YOUR COMPUTER AGAINST NETWORK ATTACKS 59

CHAPTER 10. PROTECTING YOUR MAIL FROM VIRUSES 61

CHAPTER 11. DEALING WITH VIRUSES 63

CHAPTER 12. RENEWING YOUR LICENSE 66

CHAPTER 13. DOWNLOADING UPDATES 69
13.1. When you should download updates 70
13.2. Which anti-virus database should be used 70
13.3. Downloading updates from the Internet 72
13.4. Copying updates from a local folder 73
13.5. Updating Kaspersky Anti-Virus application modules 74
13.6. Configuring proxy server parameters 75
13.7. Updater settings. Scheduled updates 77
13.8. On-demand updates 78

CHAPTER 14. ADDITIONAL SETTINGS 79
14.1. Configuring real-time protection settings 79
14.2. Configuring on-demand scan settings 80
14.3. Configuring protection against network attacks 82
14.4. Creating a list of exclusions 83
14.5. Managing quarantined objects 87
14.6. Managing backup copies of objects 88
14.7. Additional quarantine and backup storage settings 90
14.8. Managing reports 91

14.8.1 Displaying reports 95
14.8.2 Exporting and sending reports 96
14.9. Additional settings of Kaspersky Anti-Virus Personal 96
14.10. Configuring prompts for confirmation 101
14.11. Restricting the functionality of Kaspersky Anti-Virus 102
14.12. Working in the administrator and the user mode 102
14.13. Managing Kaspersky Anti-Virus configuration 103

CHAPTER 15. FREQUENTLY ASKED QUESTIONS 104

APPENDIX A. CONTACTING TECHNICAL SUPPORT 108

APPENDIX B. GLOSSARY 110

APPENDIX C. KASPERSKY LAB 116
C.1. Other Kaspersky Lab Products 117
C.2. Contact Us 122

APPENDIX D. LICENSE AGREEMENT 123

CHAPTER 1. INTRODUCTION

1.1. Computer viruses and malicious computer programs

As the number of computer users grows and the exchange of information via the Internet and email increases in volume, there is an increased threat of computer infection and data corruption or capture by malicious computer programs, also known as "malware". The most common and dangerous sources of malware penetrating users' computers are:

- **Internet**. Global information network is the main source of distribution of all types of malware. Viruses and other malicious programs can be located on internet website disguising themselves as useful software or freeware. Some scripts that run automatically run when a website is loaded in the user's browser may launch a malicious program.
- **E-mail messages**. E-mail messages that are delivered to the user's mailbox and are stored in the e-mail databases may contain viruses. Malware can be located either in the attachments to messages or in the body of a message. As a rule, infected e-mail messages contain viruses or mail worms. When you open a letter or save an attachment file to a disk, you can infect data stored in your computer.
- **Software vulnerabilities**. The so-called "holes" in software are a major source of hackers' attacks. Such vulnerabilities allow hackers to obtain remote access to your computer and therefore – to you date and LAN resources available to you and to other sources of information.
- **Removable media**. Removable media, such as removable disks, diskettes, flash-cards are used to transfer information. When you run a file located on a removable drive, you can damage data stored in your computer.

In order to be aware of the potential threats to your computer, it is helpful to know what the types of malicious software ("malware") are and how they work. In general, malicious programs fall into one of the following categories:

- **Viruses** – programs that *infect* other programs by adding their code to the infected program's code in order to gain control when infected files are run. Viruses spread somewhat slower than worms.
- **Worms** – malicious programs that belong to this category use network resources for distribution. These programs were called "worms" due to

their ability to tunnel from one computer to another, using networks and e-mail. Due to this ability, worms can proliferate extremely fast.

They penetrate a computer and send copies of themselves to other computers within the network. Apart from the network addresses, worms often use data contained in the address books of e-mail client applications installed on the infected machine.

- **Trojans** – a category of malware that are not exactly viruses as the term is usually interpreted (that is, Trojans do not infect other computer programs or data); Trojans can not penetrate computers by themselves and are distributed by intruders as some "useful" software. However, Trojans may inflict far greater damages compared to a regular virus attack.

- **Spyware** – software used to collect information a user or an organization without their knowledge. You may not even suspect that spyware is present in your computer. As a rule: spyware programs have the following purposes:

    - track actions performed by the user on the computer;

    - collect information about the content of the hard drive; in this case, most often such programs scan some folders and the system register to compile the list of software installed in the computer.

  However, such programs do not restrict themselves to the collection of the information; they impose a real threat to the security of your computer. At least two of known programs – Gator and eZula allow the intruder to control the user's computer rather than only to collect information.

- **Adware** – code that, without the user's knowledge, is included into a program's code in order to display advertising messages. As a rule, adware is integrated into freeware programs. The advertising component is located in the interface. Such programs also collect personal information about the user and transfer collected information to their developers.

- **Riskware** – software that is not a virus, but that contains a potential threat. Under some conditions, the presence of such programs on your computer imposes a threat to your data. Such programs include remote administration utilities, automatic dialers that attempt to connect user with pay-per-visit internet sites using Dial-Up connection and other programs.

- **Jokes** – software that do not inflict any direct damage to the computer but display messages declaring that the damage was inflicted or can be inflicted under certain conditions. Such programs often warn the user about a danger that does not exist, for example, they display messages about

disk formatting (that actually does not happen), “detect” viruses in files that are actually not infected.

- **Rootkit** – utilities that are used to conceal malicious activities. Rootkit utilities conceal malicious programs to prevent their detection by anti-virus software. Rootkits can modify the operating system on the computer and change its main functions in order to conceal their presence and actions performed by the intruder on the infected computer.
- **Other dangerous programs** – various programs developed to create other malware, arrange DoS attacks to remote servers, hack other computers, etc. Such programs include hacking utilities (Hack Tools), virus constructors, etc.

Henceforth in the text of this User's Guide the term "virus" will be used to refer to malicious software and the term “dangerous objects” will be used to refer to objects infected with such software. A particular type of malware will be mentioned only when it is required.

1.2. The purpose and major functions of Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal (hereinafter referred to as Kaspersky Anti-Virus or the application) is designed to provide anti-virus protection for personal computers running Windows (see section 1.4, page 12).

When installed on your computer, the application performs the following functions:

- **Protection against viruses and malicious computer programs** – the application detects and eradicates viruses that attempt to penetrate your computer. When using the application, the following two major modes can be used (either jointly or separately):
  - **Real-time anti-virus protection** – performs an anti-virus scan of all objects being run, opened or saved.
  - **On-demand scan** – performs an anti-virus scan of your entire computer or of selected disks, files, or folders. You can launch an on-demand scan manually or set up a regular scheduled scan.
- **Recovery from a virus attack** – performing a full scan and disinfection using settings recommended by Kaspersky Lab will allow you to detect any viruses that have infected your files during a virus attack.

- **Scanning and disinfecting of incoming/outgoing email traffic** – real-time protection performs a real-time anti-virus scan and disinfection of incoming and outgoing email messages[1]. In addition, the application provides on-demand scanning and disinfection of the mail databases of email clients[2] (see Chapter 10, page 61).

- **Protection of the user's computer against network attacks** – analysis of all data entering the user's computer from the network (either LAN or internet) to determine whether these data are a part of an internet attack. If an internet attack is detected, the attack will be repelled and the attacking computer will be blocked. Additionally, the application provides for the operation in the stealth (invisible) mode when the user's computer receives data from other computers only when the data exchange with the particular machine has been initiated by the user.

- **Updating of the anti-virus database, network attacks database and application modules** – updating the anti-virus database and network attacks database with information about new viruses and attacks and with methods used for disinfecting objects infected with viruses and updating the application modules (if this option is not disabled). Updates are downloaded from Kaspersky Lab's updates servers or copied from a local folder in your computer.

- **Recommendations on application setup and operation** – the application will display tips from Kaspersky Lab's experts and recommendations on the settings that correspond to the optimal anti-virus protection level.

  When a dangerous object is found, if the anti-virus database has been not updated for a critically long time, or your computer has not been scanned for a long time, the main window of Kaspersky Anti-Virus will recommend a course of actions supported with an explanation to justify such actions.

  Kaspersky Lab's experts have configured the application for optimal performance based on the extensive expertise in the anti-virus protection business, and the analysis of the feedback received by our support service from the application users. The recommended anti-virus protection settings apply immediately after you install and run the application.

- **Using various application configuration profiles** – creating and using special configuration files (profiles) that store the application's settings. You can easily alter the Kaspersky Anti-Virus configuration by specifying the application's settings and saving such changes in the profiles. For ex-

[1] The program scans only email messages received via the POP3 protocol and sent via the SMTP protocol.

[2] Kaspersky Anti-Virus® can scan email databases for any email client program, but can disinfect only Microsoft Office Outlook and Microsoft Outlook Express email databases.

ample, you can configure the application to work in the real-time protection mode only or to perform on-demand scan and then use such configurations when you feel it is necessary. You can also return to the recommended settings any time while using Kaspersky Anti-Virus.

- **Moving to quarantine** – moving objects that are possibly infected with viruses or their modifications to a special secure storage area. You can then disinfect or delete any quarantined object, restore it to its initial location or send it to Kaspersky Lab for analysis. Quarantined files are stored in a special format and do not impose any threat to your computer.
- **Creating backup copies of objects** – creating backup copies of objects in a special backup storage prior to disinfection or deletion of such objects. Such copies are created for the cases when it is necessary to restore an original object if it contains valuable information or in order to restore the infection situation for analysis purposes. Backup copies are stored in a special format and do not impose any threat.
- **Reporting** – results of all actions performed by Kaspersky Anti-Virus are documented in reports. A detailed scan report contains statistics of all scanned objects, stores information about settings used for each task and the history of actions performed on each individual file. Reports are also generated during real-time protection, and after updating the anti-virus database and application modules.

1.3. What's new in Version 5.0?

Kaspersky Anti-Virus Personal 5.0 has the following features not found in Version 4.5:

- *Maintaining scanned objects database*. Version 5.0 does not scan previously analyzed objects that have not changed since the time they were last scanned. This applies both to real-time protection and to the on-demand scan. This feature greatly improves the application's speed and performance.
- *Scanning and disinfecting incoming and outgoing mail* for any email client that receives mail using the POP3 protocol and sends mail using the SMTP protocol. The previous version protected only mail sent and received by Microsoft Outlook.
- *Disinfecting infected archives*. Version 5.0 disinfects infected files in zip, arj, cab, rar, lha and ice archives. The previous version provided detection and disinfection of infected files in zip archives only.

Kaspersky Anti-Virus only scans multi-volume archives in the formats listed above and self-extracting archives, but does not disinfect them.

- *Protection against network attacks*. This version of Kaspersky Anti-Virus protects your computer against currently widespread network or hacking attacks.
- *Intuitive user-friendly interface*. This version is a single application, whereas the previous release consisted of several components each performing their own anti-virus protection functions. This new approach simplifies control over the most important Kaspersky Anti-Virus functions. For example, the anti-virus protection level can be set by simply moving a slider rather than editing settings.
- *Recommended settings and experts' tips*. To simplify application operation, the default settings of this version of the application match the settings recommended by Kaspersky Lab and in most cases there is no need to configure the application before use. When the anti-virus protection level is set to High Speed, the user is prompted to switch to a higher level of anti-virus protection.
- *Application operation profiles management*. A possibility to store the application's settings in a special file so that you can use them any time later. If you are not satisfied with the recommended Kaspersky Anti-Virus settings, configure the application based on your requirements and save this configuration in a *profile* file.
- *Product license renewal*. Users of Version 5.0 can now install a new license key, extending the license period.
- *Sending your files for analysis to Kaspersky Lab*. Now you can send us possibly infected files detected by Version 5.0 or files that you suspect may be infected.
- *The ability to delete infected composite objects has been removed*. You cannot inadvertently delete infected composite objects (archives, email clients' databases or email format files) using Version 5.0. However, you can still delete such objects using standard Windows tools such as Windows Explorer. The exception is self-extracting archives.
- *Prohibition of infected email databases deletion*. Now the infected email databases cannot be deleted by means of Kaspersky Anti-Virus. However you still can delete the given objects manually.
- *Access to the Kaspersky Anti-Virus settings is now password-protected*. You can setup a password that will be asked for by the application every time when switching between the user's and the administrator's mode. The user's mode does not allow modification of the application's settings,

disabling the real-time protection and closing Kaspersky Anti-Virus Personal on your computer.

1.4. Hardware and software system requirements

For normal performance of Kaspersky Anti-Virus Personal 5.0, your computer must meet the following minimum requirements:

General Requirements:

- 50 MB available space on your hard drive
- CD-ROM drive (for installation of Kaspersky Anti-Virus from CD) or floppy drive (for installation from floppy disks, and to read license key)
- Microsoft Internet Explorer 5.5 or higher (for updating anti-virus database and application modules via the Internet)

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service pack 6a):

- Intel Pentium 300 MHz processor or higher
- 64 MB RAM

Microsoft Windows 2000 Professional (Service Pack 2 or later), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 or later):

- Intel Pentium 3000 MHz processor or higher
- 128 MB RAM

1.5. Distribution Kit

You can purchase Kaspersky Anti-Virus either from our dealers (retail box) or online (for example, you may visit http://www.kaspersky.com, and go to **E-Store** section).

The contents of the retail box package include:

- Sealed envelope with an installation CD, or set of floppy disks, containing the application files.
- User's Guide.
- License key written on a special floppy disk.

- License Agreement.

Before you open the envelope with the CD (or a set of floppy disks) make sure that you have carefully read the license agreement.

If you buy Kaspersky Anti-Virus online, you will download the application from the Kaspersky Lab website. In this case, the distribution kit will include this User's Guide along with the application. The license key will be emailed to you upon the receipt of your payment.

The License Agreement is a legal contract between you and Kaspersky Lab that describes the terms and conditions under which you may use the anti-virus product that you have purchased.

Please read the License Agreement carefully!

If you do not agree with the terms and conditions of the License Agreement, return the retail box to the Kaspersky Anti-Virus dealer you purchased it from and the money you paid for the product will be refunded to you on the condition that the envelope with the installation CD (or set of floppy disks) is still sealed.

By opening the sealed envelope with the installation CD (or set of floppy disks), you confirm that you agree with all the terms and conditions of the License Agreement.

1.6. Services provided for registered users

Kaspersky Lab offers all registered users an extensive service package enabling them to use Kaspersky Anti-Virus more efficiently.

After purchasing a license you become a registered user and during the license period you can enjoy the following services:

- application module and anti-virus database updates;
- support on issues related to the installation, configuration and use of the application. Services will be provided by phone or via email;
- information about new Kaspersky Lab products. You can also subscribe to the Kaspersky Lab newsletter which provides information about new computer viruses as they appear.

Kaspersky Lab does not provide support on issues related to the performance and the use of operating systems or other technologies.

CHAPTER 2. INSTALLING THE APPLICATION ON YOUR COMPUTER

To install Kaspersky Anti-Virus on your computer, run the executable file from the installation CD.

Installation of the application using the distribution kit downloaded from the internet is identical to the installation from the distribution kit on CD.

The installation wizard operates in the interactive mode. Each dialog box has the following buttons that you can use to navigate through the installation process:

- **Next>** – accept and proceed with the installation.
- **<Back** – return to the previous stage of the installation process.
- **Cancel** – cancel the application installation.
- **Finish** – finish the application installation.

A detailed discussion of each step of the installation process is provided below.

Step 1. Checking the version of the operating system installed on your computer

Before the installation of the application, the operating system and Service Packs installed on your computer are checked for the conformity with the minimum system requirements for the installation of Kaspersky Anti-Virus Personal.

Should the application determine that any of the requirements is not met, the corresponding notification will be displayed. We recommend that you install the required programs and Microsoft Windows update packages using **Windows Update** (or other utilities) before proceeding with the installation of Kaspersky Anti-Virus Personal.

Step 2. Searching for other anti-virus software

The next step involves a search for other installed anti-virus software (including Kaspersky Lab applications). This is performed because the simultaneous use of these applications with Kaspersky Anti-Virus may cause conflicts.

If an earlier version of Kaspersky Anti-Virus is found (as for example version 4.5), you will be asked if you would like to keep the license key for this product if such license key is still valid.

We recommend that you keep the valid license key that was used earlier as this key can be used with Kaspersky Anti-Virus Personal 5.0.

After you save the key, you will be prompted to uninstall the earlier version of the product as it is in conflict with Kaspersky Anti-Virus Personal 5.0.

Click **OK** button in order to abort the installation. After this uninstall the earlier version of Kaspersky Anti-Virus and run the product installation wizard again.

If during the previous step you saved a valid license key used for Kaspersky Anti-Virus 4.x to be used in version 5.0, then the license key installation window will not be displayed during the installation procedure (see Step 8 on page 17). The key will be used for the program operation.

If any anti-virus software from a different vendor is found installed on your computer, you will be prompted to uninstall this program before proceeding with the installation of Kaspersky Anti-Virus.

We recommend that you uninstall such program(s). To do this, click the **No** button, in order to abort the installation. Then uninstall the program and run the product installation wizard again.

Kaspersky Lab's specialists do not recommend installing several anti-virus products on one computer as their joint use may cause conflicts.

If it is determined that Kaspersky Anti-Virus Personal 5.0 has already been installed on your computer, a message will be displayed with a warning that if you proceed with the installation, the application that was installed earlier will be updated by the new installation.

If you are upgrading version 5.0, the license key installation window (see Step 8 on page 17) will not contain information about they key, but the key installed earlier will be used for the program operation.

Step 3. Start the Installation Wizard

If no other anti-virus software is found installed on your computer, immediately after the executable file is run, an installation startup window will appear to inform you that the installation of Kaspersky Anti-Virus Personal on your computer has begun.

To proceed with the installation, click **Next>**. To cancel the installation, click **Cancel**.

Step 4. Read the license agreement

The next dialog box contains a License Agreement between you and Kaspersky Lab. Read it carefully and click **I Agree** if you agree with all terms and conditions of the Agreement. The installation process will continue.

Step 5. Provide user information

At this point the user name and the user's company name will be determined. Default information will be copied from the operating system registry. You can alter it if you wish.

To proceed with the installation, click **Next>**.

Step 6. Read important information about the application

During this stage of the installation process you will be asked to read important information about the application before you start using Kaspersky Anti-Virus.

This dialog box contains information about the major features and functionality of Kaspersky Anti-Virus.

Here you can also define whether you want the program to use setting recommended by the Kaspersky Lab's experts. These settings determine the speed of Kaspersky Anti-Virus operation and the degree of the information protection on your computer.

By default this mode is enabled. If you plan to use settings other than the recommended settings, uncheck the **Operate according to recommended settings** box.

In order to proceed to the next step of the setup process, click **Next >**.

Step 7. Using the proprietary Kaspersky Lab's technology

This step of the setup process is performed only if you have unchecked the **Operate according to recommended settings** checkbox during the previous step.

During this step of the Kaspersky Anti-Virus setup process you will have to make a decision whether you want the program to use the following technologies:

Real-time protection against network attacks – technology used to protect your computer against hackers attacks. This technology protects your computer against network attacks and prevents corruption, theft of or unauthorized access to your data. By default the real-time protection against network attacks is enabled. In order to disable real-time protection, uncheck the **Use real-time protection against network attacks** checkbox. You can enable/disable the real-time protection against network attacks later, while using the program (see Chapter 9, page 59).

iStreams™ Technology – an anti-virus scan acceleration technology (details see Appendix B, page 110). In order to disable this technology, uncheck the ☑ **Use the iStreams™ technology** checkbox.

This technology can be used on computers with the NTFS file system only.

If you disable the use of the iStreams technology at this stage, you will have to re-install Kaspersky Anti-Virus in order to enable it later.

In order to proceed with the setup process, press **Next>**.

Step 8. Install the license key

Perform this step only if the Kaspersky Anti-Virus Installation Wizard fails to find the key file automatically

During this step, the license key for Kaspersky Anti-Virus will be installed. The license key is your personal "key" that stores all service information required for proper full-featured operation of the application, including the following reference information:

- Technical support information (support service provider and contact information).
- License name, number, and expiry date.

The application will not work without the license key.

In order to install a license key,

1. Press the **Browse** button and browse to the folder containing the license key file:
   - If you purchased a retail box version of Kaspersky Anti-Virus, you will find the license key written or a special floppy disk. You will have to insert the disk into the drive and select this drive (see Figure 1).

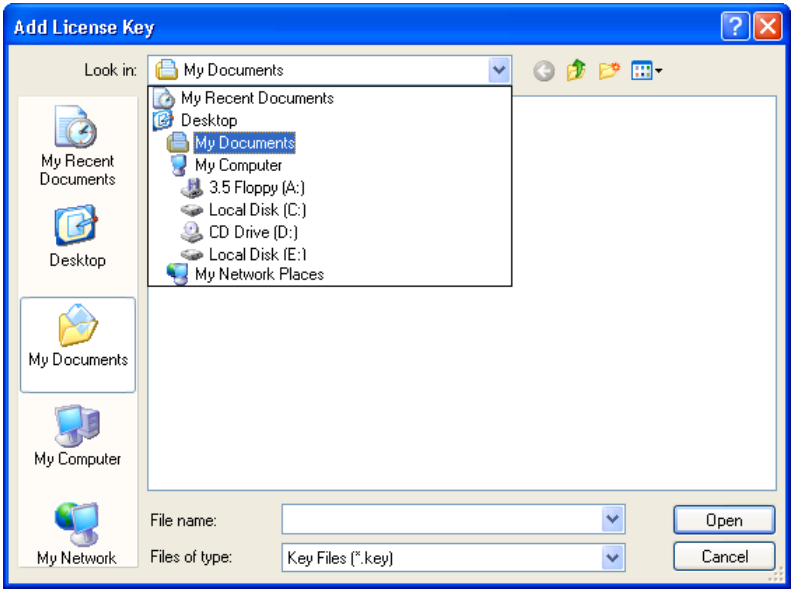

Figure 1. Selecting path to the license key file

- If the license was purchased online, then the license key file that you received by via e-mail shall be saved in any folder on your computer's hard drive. You will have to open this folder.

The selected folder will display the list of available license keys.

2. Select the required license key (a file with .**key** extension) and press the **Open** button (see Figure 2).

As the result, the installation wizard will display general information about the license and the path to the license key file.

In order to proceed with the installation press **Next >**.

If you do not have the license key at the time of installation (for example, if you ordered it via the Internet but have not received it yet), you may install it later, when you run the application for the first time or using a special license key installation utility (see Chapter 12 on page 66). Remember that you cannot start using Kaspersky Anti-Virus without the license key.

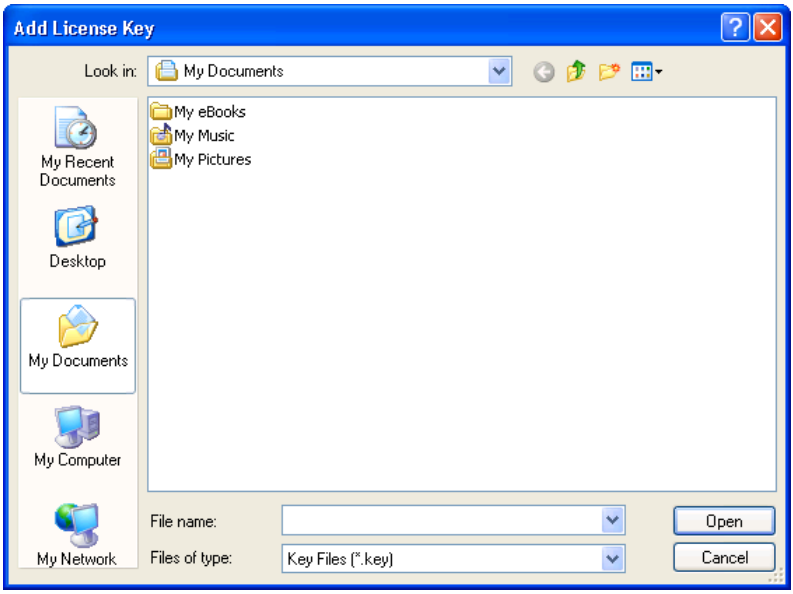

Figure 2. Selecting the license key file

Step 9. Select the installation folder

During this step, the destination folder will be selected for the installation of the application files. The default path is: **<Disk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Personal**.

You can type in the path to this folder or press the **Browse** button and use the standard **Select Folder** dialog box to locate and select the folder.

If you are updating from a previous version of Kaspersky Anti-Virus Personal, you will be offered to perform the new installation into the existing folder as the recommended option. You can specify a different folder; in this case the application files of the previous installation will remain on your hard driver and can only be deleted with the full application removal.

Press the **Install** button in order to proceed with the installation. After this, Kaspersky Anti-Virus application files will be copied to your computer.

Step 10. Finish setup

A **Completing the Setup** dialog box informs you that installation of Kaspersky Anti-Virus on your computer has been completed.

If registration of system services is required, you will be asked to restart your computer. This is a MANDATORY step for the correct completion of the application installation.

To complete the setup:

1. Choose one of the following options:
   - **Yes, I want to restart my computer now**
   - **No, I will restart my computer later**
2. Click **Finish**.

If your computer does not need to be restarted to complete the setup, you can begin using the program immediately. Perform the following steps to finish the installation:

1. If you do not want to enable anti-virus protection of your computer immediately after the installation is completed, uncheck the ☑ **Run Kaspersky Anti-Virus Personal 5.0** box.

   If you uncheck this box, the anti-virus protection of your computer will be automatically enabled after reboot. Before this time you can manually enable anti-virus protection from the Windows main menu (**Start → Programs → Kaspersky Anti-Virus Personal**).
2. Click the **Finish** button.

As a result of installation and launch of Kaspersky Anti-Virus:

- The application icon will be added to the system tray
- Application shortcuts will be added to the main Windows menu (**Start → Programs → Kaspersky Anti-Virus Personal**).

CHAPTER 3. IF YOUR COMPUTER IS INFECTED...

Sometimes it is not apparent, even to a knowledgeable user, that a computer is infected with a virus because viruses efficiently camouflage themselves among regular files. This chapter contains a detailed discussion of the signs of a virus infection, methods of data recovery after a virus attack and measures aimed at prevention of data corruption by viruses.

3.1. Signs of infection

There are a number of signs indicating that your computer has probably been infected. If you are noticing "strange things" happening to your computer, for example:

- unexpected messages or images are suddenly displayed;
- unusual sounds or music played at random;
- your CD-ROM tray mysteriously opens and closes;
- programs suddenly start on your computer;
- if Kaspersky Anti-Hacker is installed on your computer, it notifies you of attempts by some programs to connect to the Internet although you did not initiate this.

If you notice any of the above signs, it is very likely your computer has been infected with a virus.

In addition, there are some typical signals indicating that your computer has been infected via email:

- your friends mention that they receive messages although you never sent such messages;
- your mailbox contains many messages without the sender's email address or header.

Note that these problems may be caused by reasons other than viruses. For example, infected messages, which have your address as the sender, could have actually been sent from a different computer.

There are also indirect signals indicating that your computer is possibly infected:

- your computer freezes frequently or encounters errors;
- your computer slows down when programs are started;
- you are unable to load the operating system;
- files and folders are suddenly missing or their content changes;
- your hard drive is accessed too often (the light on your main unit flashes rapidly);
- Microsoft Internet Explorer "freezes" or displays unpredictable behavior, (for example you cannot close the application window).

In most cases such indirect signs indicate that there is a hardware or software problem, but although such signs are unlikely to be caused by an infection, we recommend that you perform a full scan of your computer using the default settings recommended by Kaspersky Lab experts if your encounter any of these problems.

3.2. What should you do if you notice symptoms of infection

If you notice that your computer displays "suspicious" behavior:

1. Don't panic! This golden rule may prevent the loss of important data stored on your computer and help you avoid unnecessary stress.
2. Disconnect your computer from the Internet.
3. If your computer is connected to a Local Area Network, disconnect it.
4. If the symptom of an infection is that you cannot boot from your hard drive (your computer encounters an error at startup), try to start the system in Safe Mode or from the Windows boot disk that you created during the installation of the operating system on your computer.
5. Before taking any action, back up all critical data to an external drive (a floppy disk, CD, flash card, etc.)

Later, before you move saved data to the computer after it has been disinfected, make sure that you have scanned this data with Kaspersky Anti-Virus (see Chapter 7 on page 51).

6. Install Kaspersky Anti-Virus.
7. Download the latest anti-virus database updates. If possible, do not use the infected computer to download the updates, but instead use a friend's computer, or a computer at your office or an Internet café. It is preferred that you use a different computer because when you connect to the internet using an infected computer some important information stored on your computer may be sent to the malefactors or the virus may be sent to the contacts stored in your address book. Therefore, if you suspect an infection it is the best to immediately disconnect from the Internet and from any local area network you are connected to. You can also obtain the anti-virus database on a CD-ROM or a floppy disk from Kaspersky Lab or its authorized dealers and update your databases from this disk (for more details see section 13.4, page 73).
8. Apply the recommended application settings (see section 6.2, page 39).
9. Perform a full system scan (see section 6.3, page 44).

CHAPTER 4. ANTI-VIRUS PROTECTION USING KASPERSKY ANTI-VIRUS DEFAULT SETTINGS

You can use Kaspersky Anti-Virus immediately after the installation is complete. There is no need to customize the application before its first use because the default settings provide the optimal balance between the extent of protection of your computer and its performance.

Operation of Kaspersky Anti-Virus with the recommended settings applied is discussed in detail below.

4.1. Real-Time Protection

Real-time protection is enabled from the moment your operating system has started until you turn off your computer. This is indicated by the red icon in they system tray. Immediately after the system is started, Kaspersky Anti-Virus scans *its own application modules, RAM* and all *startup objects*. Then the application performs the scan of objects being opened, saved or run.

By default the real-time protection uses settings recommended by the Kaspersky Lab's experts, namely:

- Objects being opened, saved or executed on your hard drive and removable drives that are potentially infectable will be scanned, including:
    - *disk boot sectors* (these objects are scanned immediately after the system startup);
    - *packed files* and objects linked to or embedded into files *(OLE objects);*
    - incoming email messages.

Real-time protection does not scan objects that cannot contain viruses.

- When an infected object is detected, the application denies access to this object and prompts the user for action.

- When a suspicious or infected object is detected, the application denies access to it and prompts the user for action.
- When a *network* attack is detected, the application displays a corresponding message and blocks the attack.
- The results of all application actions are documented in reports (see section 14.8, page 91).

The real-time protection can be disabled for a certain period of time or altogether. Kaspersky Lab's experts strongly recommend that you do not disable the real-time protection as it considerably increases the risk of infecting your computer. If you need to disable the real-time protection of your computer for some reason, disable it temporarily.

In order to disable real-time protection temporarily,

1. Right-click the icon in the system tray.
2. When the shortcut menu appears, select **Stop Real-Time Protection**.
3. In the window used to disable real-time protection, select the period of time during which you wish the real-time protection of your computer to be disabled. Details on disabling real-time protection see section 8.3, page 57).

Real-time protection of your computer will be then stopped and the active icon (red) will be replaced by the inactive icon (gray color) to indicate this change.

4.2. On-Demand Scan

The **on-demand scan** feature is designed to perform anti-virus analysis of your entire computer or of specified disks, folders or files. By default the scan is performed using settings recommended by the Kaspersky Lab's experts as follows:

- an on-demand scan of your entire system will scan *RAM used for the running processes* and all objects stored on hard drives, including:
  - *startup files and disk boot sectors;*
  - *archives, packed executable files and self-extracting archives;*
  - objects linked to or embedded into files (*OLE objects)*;

The full computer scan does not include the analysis of mailboxes that are currently in use.

- an anti-virus scan of a particular disk, folder or file will scan all files located within the selected area, including:
  - *archives*, *packed executable files* and *self-extracting archives*;
  - objects linked or embedded into files (*OLE objects*);
- dangerous objects are processed after the scan is complete; possible actions will be listed for each object;
- the results of all application actions are documented in reports (see section 14.8, page 91).

By default, a full on-demand scan of your computer is scheduled every Friday at 8 pm. The full scan status indicator (see Figure 5) is located in the right section of the **Protection** tab.

The full scan of your computer is in progress

If your computer is off at the scheduled time, the scan will not be performed.

You can start a full scan of your computer manually. To do this:

right-click the icon in the system tray. When the shortcut menu appears, select **Scan My Computer for viruses**.

or

switch to the **Protection** tab in the application window and follow the Scan My Computer hyperlink in the left section.

4.3. Updating the anti-virus database

The application detects viruses and disinfects dangerous objects using the anti-virus database that contains definitions of all currently known viruses and methods for disinfection.

It is extremely important to update your anti-virus database periodically because new viruses appear every day.

Updating anti-virus database is an important function of Kaspersky Anti-Virus. By default, database updates are automatically downloaded from the Kaspersky Lab's update servers and installed on your computer every 3 hours. If you use your computer less than three hours a day, the anti-virus database will be updated immediately after Kaspersky Anti-Virus is launched.

You can update the anti-virus database manually. To do this:

right-click the icon in the system tray. When the shortcut menu appears, select **Update Anti-Virus Database**.

or

open the **Protection** tab (see Figure 5) of the main application window and follow the Update now hyperlink in the left section.

or

click hyperlink Update your anti-virus database in the right section of the **Protection** tab.

For more details on updating the anti-virus database see Chapter 13, page 69.

CHAPTER 5. APPLICATION INTERFACE

Kaspersky Anti-Virus has an intuitive easy-to-use interface. This chapter contains a discussion of the main elements of the application interface: system tray icon, shortcut menu, main application window and the service windows.

5.1. System tray icon

After the application is started, an icon indicating the status of real-time protection will appear in the Windows system tray.

If the application icon is enabled (red color) , this means that all files on your computer are monitored by Kaspersky Anti-Virus. If the icon is disabled (grey color) , it means that the real-time file protection is disabled (for example, if you have temporarily or permanently disabled real-time file protection).

When the application is scanning an object, the lower right-hand corner of the icon becomes a flashing white-and-blue folder: or . When mail is being scanned, an envelope will be displayed instead of the folder - . When the updates are being downloaded, icon will be displayed.

If the system tray icon animation is disabled in Kaspersky Anti-Virus additional settings (see section 14.9 on page 96), the icon will only have two states: enabled or disabled.

When an important anti-virus event occurs, the recommended action will be indicated in a pop-up window above the icon (see Figure 3).

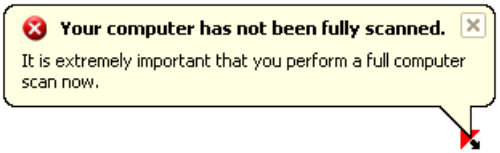

Figure 3. Information message

5.2. Shortcut menu

To open a shortcut menu, right-click the application icon in the system tray (see Figure 4). The menu includes the following items:

- **Open Kaspersky Anti-Virus** – open the main application window with the **Protection** tab active. You can also open the main window by clicking the icon in the system tray.

Figure 4. Shortcut menu

- **Switch to user/administrator mode** – switch from one security mode to another.
- **Scan My Computer for viruses** – perform a full scan of your computer for viruses using the selected protection level settings.
- **Update Anti-Virus Database** – download updated anti-virus database.
- **Resume/Stop Real-Time Protection** – enable or temporarily disable real-time protection of your computer. The application icon in the system tray changes color depending on whether real-time protection is disabled or enabled.

We do not recommend that you stop real-time anti-virus protection because this considerably increases the risk of virus infection of your computer.

- **About** – display general information about Kaspersky Anti-Virus Personal.
- **Exit** – close Kaspersky Anti-Virus.

5.3. Main application window: general layout

The main application window allows quick access to all the application's anti-virus protection capabilities. Using the main application window, you can:

- configure the anti-virus protection settings;
- start and stop a scan of the entire system or specified disks, folders or files for viruses;
- download updates for the anti-virus database, network attacks database and application modules;
- set up schedules for full scans and automatic updating;
- manage quarantined objects;
- manage object copies created in the backup storage before the attempt to disinfect or delete such objects;
- manage reports, etc.
- manage the application's configuration, etc.

All anti-virus protection settings, status information and specific tasks are accessible from the following tabs of the main window:

- **Protection** tab – a main window tab that displays the anti-virus protection tasks (objects scan and anti-virus database updating) and their status. From this tab you can switch to quarantine, backup storage and reports. This tab will always open first when you start using the application (see section 5.3.1, page 32).
- **Settings** tab – a main window tab that displays the settings and status for all anti-virus tasks (see section 5.3.2, page 33).
- **Support** tab – a tab where you can view information about the license key, renew the application license, access online Help system and send questions to the Technical Support Service (see section 5.3.3, page 34).

Each tab has two sections as follows:

- *The left section* displays hyperlinks that you can use to perform tasks required during the operation of Kaspersky Anti-Virus. Each tab has its own list of specific tasks.

  For example, the **Protection** tab offers a variety of tasks related to the anti-virus scanning function. The **Settings** tab includes hyperlinks used to

adjust settings for these tasks. The **Support** tab includes tasks that support your anti-virus protection.

- *The right section* contains information on the current status of the anti-virus protection of your computer, including real-time protection, on-demand scan, anti-virus database and license information.

  Thus, for instance, the **Protection** tab displays the status of your anti-virus protection, the **Settings** tab displays the status of the current application settings and the **Support** tab displays the license status (license key information), support contact information and information about the application and your system.

Four states of anti-virus protection are indicated in the **Protection** and the **Settings** tabs by the following icons:

Critical level of anti-virus protection. This status means that the real-time protection is disabled or that certain tasks (scanning and/or updating) have not been performed for a long time or that the current settings do not provide reliable anti-virus protection of your computer.

Anti-virus protection is stopped. This status indicates that the protection of your computer is temporarily disabled.

Anti-virus protection level does not match the recommended settings. This status indicates that current anti-virus protection settings do not match the recommended settings or that a certain anti-virus protection task must be performed.

The anti-virus protection level is set to Recommended. This status indicates that your settings fully comply with the settings recommended by Kaspersky Lab.

The status information is displayed in the following order: the real-time protection status, the on-demand scan status, and, finally, the status of the anti-virus database validity.

Each state described above is provided with comments and recommendations. Thus, for example, if the current anti-virus protection level does not match the recommended level, you will be prompted to restore the recommended settings to ensure the optimal protection level.

5.3.1 Protection tab

Using the **Protection** tab (see Figure 5), you can scan your entire computer or individual disks, folders or files. You can also:

- launch the updating of the anti-virus database, application modules and network attacks database;
- switch to progress reports on all running tasks (view, delete, export to a file);
- switch to managing quarantined objects that are possibly infected with a virus or a virus modification;
- switch to managing backup copies of disinfected or deleted objects.

These tasks can be launched by clicking the corresponding hyperlinks.

In the right section of the tab, you can view the *current status of real-time protection, on-demand scan and anti-virus database*. An example (see Figure 5) shows that real-time protection is enabled but a full scan has not been performed for a long time. Here you can also view comments on the status of each anti-virus protection task.

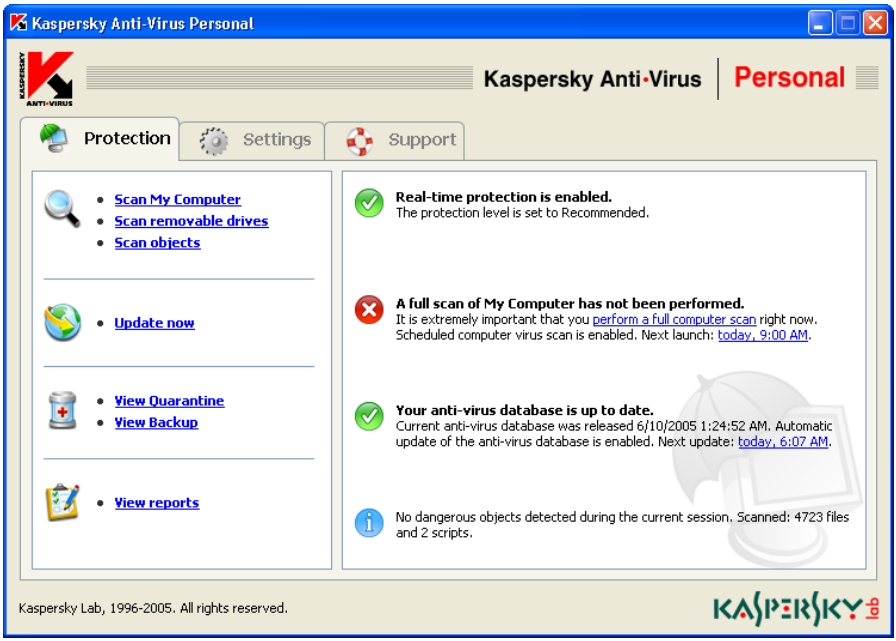
Kaspersky Anti-Virus Personal
Kaspersky Anti-Virus
Personal
Protection
Settings
Support
Scan My Computer
Scan removable drives
Scan objects
Update now
View Quarantine
View Backup
View reports
Real-time protection is enabled.
The protection level is set to Recommended.
A full scan of My Computer has not been performed.
It is extremely important that you perform a full computer scan right now.
Scheduled computer virus scan is enabled. Next launch: today, 9:00 AM.
Your anti-virus database is up to date.
Current anti-virus database was released 6/10/2005 1:24:52 AM. Automatic update of the anti-virus database is enabled. Next update: today, 6:07 AM.
No dangerous objects detected during the current session. Scanned: 4723 files and 2 scripts.
Kaspersky Lab, 1996-2005. All rights reserved.
KASPERSKY lab

Figure 5. The **Protection** tab

If the protection status is critical or does not match the recommended settings, you will be prompted to modify the current settings, restore the recommended settings, or launch a certain task. The recommendations are organized as hyperlinks so that you can easily perform the corresponding action.

You can review the application's performance statistics in the lower part of the **Protection** tab. The information includes the total number of objects scanned during the current session and the number of dangerous objects detected.

5.3.2 *Settings* tab

Using the **Settings** tab (see Figure 6) you can evaluate and customize both the standard and advanced settings to ensure smooth performance of Kaspersky Anti-Virus.

The right section of the tab displays the current settings for real-time anti-virus protection, on-demand scans, and automatic updating of the anti-virus database, application modules and the known network attacks database. It also gives detailed comments and tips from Kaspersky Lab on how to customize these settings. For example, if you updated your anti-virus database manually in the past, you will be prompted to schedule automatic updates.

Kaspersky Anti-Virus Personal
Kaspersky Anti-Virus
Personal
Protection
Settings
Support
Threats and exclusions
Configure Real-Time Protection
Configure On-Demand Scan
Configure Updater
Configure Quarantine&Backup
Additional Settings
Managing profiles
Recommended Real-Time Protection settings are in use.
Upon virus detection, block access and prompt user for action.
Protection level: Recommended.
You can modify Real-Time Protection settings.
Recommended On-Demand Scan settings are in use.
Prompt user for action once the scan is completed
Scan level: Recommended.
You can modify On-Demand Scan settings.
Automatic update is enabled.
Update frequency - every three hours.
You can modify settings to select the required automatic update interval.
Kaspersky Lab, 1996-2005. All rights reserved.
KASPERSKY lab

Figure 6. The **Settings** tab

By clicking hyperlinks located in the left section of the **Settings** tab, you can edit the settings for real-time protection, on-demand scans, and anti-virus database updating. You can also create the list of objects that will be excluded from the scan scope and specify the type of the anti-virus database used.

Here you can also customize settings related to the quarantine where suspicious objects are placed as well as the settings of the backup storage used to keep backup copies of objects. Finally you can customize additional settings by following the hyperlink Additional Settings.

Kaspersky Anti-Virus offers a possibility to the user to create various working configurations and save them into special configuration files called *profiles*. Later you can easily return to the configuration you need by simply loading the required profile without the need to configure the application manually. You can switch to creating and loading profiles using the Managing profiles hyperlink.

5.3.3 *Support* tab

The **Support** tab (see Figure 7) displays contact information for Kaspersky Lab's Technical Support and how to obtain assistance when you encounter problems with Kaspersky Anti-Virus operation. The right section of the tab displays information about the application, the license key and the computer's operating system so that you can provide this information to Technical Support if required.

Kaspersky Anti-Virus Personal
Kaspersky Anti-Virus
Personal
Protection
Settings
Support
Send question to tech support
Send file for analysis
License Keys
License Renewal
Help
Virus Encyclopedia
Kaspersky Lab's Website
Support
Should you have any questions regarding the use of this application, you can contact Technical Support Service use our Knowledge base or Kaspersky Lab Forum.
Product Info
You have Kaspersky Anti-Virus Personal 5.0 installed. Current anti-virus database was released today (14.02.2006 9:44:46) and contains 165868 records.
License Info
You are currently using license key which will expire 19.01.2007 2:59:59. You can prolong license period and install new license key.
System Info
Operating System: Microsoft Windows XP, Service Pack 2
Kaspersky Lab, 1996-2006. All rights reserved.
KASPERSKY lab

Figure 7. The **Support** tab

By following the hyperlinks in the left section of the tab, you can:

- send your questions and objects possibly infected with viruses or their modifications to Kaspersky Lab's Technical Support;
- renew the license for Kaspersky Anti-Virus Personal.

The left section of the tab also includes the following reference hyperlinks:

- Help – general application reference.
- Virus Encyclopedia – a hyperlink to www.viruslist.com website that contains detailed description of all currently known malware.
- Kaspersky Lab's Website – a hyperlink to the Kaspersky Lab's website.

5.4. Scan window

After you launch an anti-virus scan of all or part of your computer, the scan window will appear (see Figure 8).

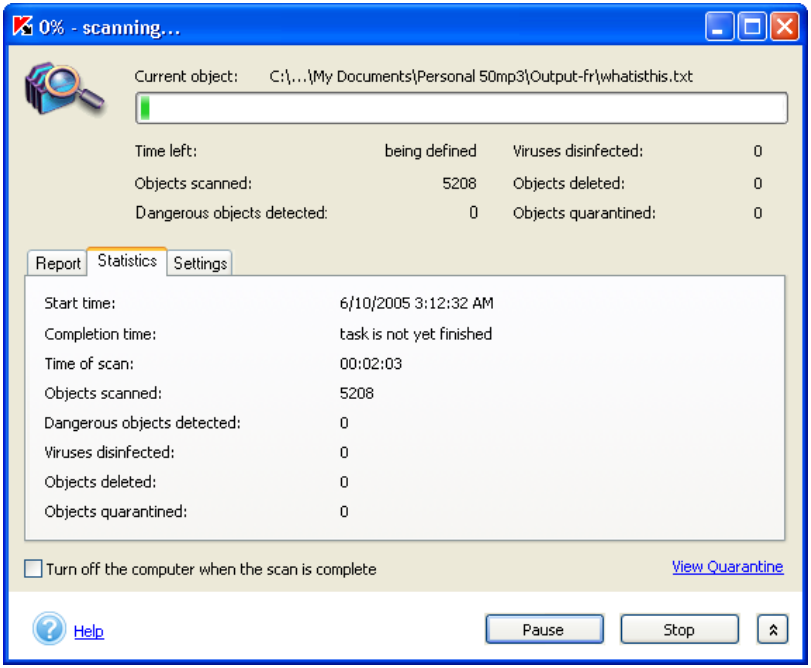

Figure 8. The **Scan** window

The scan window consists of two parts:

- the top part of the window contains a scan progress bar showing the percentage of scan progress, the name of the object currently being scanned, the estimated time of the scan completion and the general statistical data about the objects scanned, disinfected, deleted and quarantined by the moment.
- the bottom part of the window is opened by clicking the button. It contains three tabs: **Statistics**, which displays the scan results; **Report**, which contains a report on the events that occurred during the scan; and **Settings**, which contains the list of settings used for the current scan or for the last scan performed. You can then hide the bottom part by clicking the button.

See section 14.8, page 91 for report details.

If you perform a full computer scan, then using this window you can enable the automatic computer turn-off after the scan is complete. This mode is convenient if you start the computer scan at the end of your business day and do not want to wait until the scan is complete to turn off your computer manually.

However, this mode requires the following additional preparation: before you launch the scan you will have to disable prompting for password when scanning objects (if it is enabled) (see section 14.2, page 80), setup the automatic processing mode for dangerous objects, their deletion, quarantining or recording information about them into the reports (see section 6.2 page 39). These actions will disable the interactive mode of the program operation and the program will not display prompts that interrupt the scanning process.

In order to automatically turn-off your computer after the scan is complete, check the corresponding checkbox in the scan window.

5.5. Application reference system

Comprehensive application reference information is available from the **Support** tab of the main application window by simply following the Help hyperlink in the left section of the tab.

If you have a question on a particular dialog box, press the **<F1>** key or click Help in the left bottom corner of this dialog box.

CHAPTER 6. PREVENTING VIRUS INFECTIONS

Even proven and trusted preventative actions cannot ensure 100% protection against computer viruses and Trojans, but you can considerably lower the risk of being affected by a virus attack and thus reduce the losses from a possible infection if you develop and follow certain rules.

Similar to health care, one of the main methods of fighting viruses is the *prevention* of infection. For computers, prevention of a virus infection includes a few rules that must be followed to reduce the risk of infection and data loss.

Listed below are the main security rules that you should follow to prevent virus attacks.

Rule 1: *keep your computer protected with an anti-virus program and Internet security software.* To do this*:*

- Install Kaspersky Anti-Virus Personal.
- Update your anti-virus database on a regular basis. During periods of virus outbreaks you should retrieve updates several times each day because during such periods the anti-virus database on Kaspersky Lab's update servers is updated constantly.
- Apply the real-time protection settings recommended by Kaspersky Lab. Real-time protection is enabled immediately after system startup and prevents the penetration of viruses into your computer.
- Apply the on-demand scan settings recommended by Kaspersky Lab and schedule the scan to be run at least once a week.
- We also recommend that you install Kaspersky Anti-Hacker for comprehensive computer protection while you are surfing the Internet.

Rule 2: *b*e careful when copying any new data to your computer:

- Always scan all removable drives (floppy disks, CD-ROM drives, flash cards, etc.) for viruses before using them.
- Be careful with email messages. Never open an email attachment, even if it was sent to you by a person you know, unless you are expecting it. In particular, do not trust emails that claim to be sent by anti-virus companies.

- Be careful with any data downloaded from the Internet. If you are prompted to download a program, always check that it comes with a security certificate.
- If you download an executable file from the Internet or from a LAN, scan it with Kaspersky Anti-Virus.
- Be selective about the websites you visit. Some websites contain dangerous scripts or Internet worms.

Rule 3: Read carefully all information supplied by Kaspersky Lab.

In most cases, Kaspersky Lab warns users about new virus outbreaks long before they reach their peak. The risk of getting infected is still low at this time and if you download the up-to-date anti-virus database, you will be able to protect your computer.

Rule 4: Be suspicious about hoax virus warnings - email messages that claim to be warnings of virus threats.

Rule 5: Regularly update your operating system using the Windows Update utility.

Rule 6: Always buy licensed copies of your software from authorized dealers.

Rule 7: Limit the number of people who have access to your computer.

Rule 8: Reduce the potential losses from a possible infection by performing the following:

- Backup your data on a regular basis, so that in the event of data loss, your system can be restored fairly quickly using backup copies. Your distribution disks, floppy disks and other media with software installation and other important data should be kept in a safe place.
- Always create a bootable rescue disk from which you can boot using a "clean" operating system.

6.1. When do I need to perform an anti-virus scan?

Kaspersky Anti-Virus can perform an anti-virus scan of your entire computer or of a particular disk, folder, file or email object, system memory, startup objects and disk boot sectors.

During a full computer scan, mailboxes, removable drives and network drives, if such are connected to your computer, will not be scanned.

Even if, as a result of an on-demand scan of selected objects, no viruses are found, this does not guarantee that your computer is virus-free. Therefore, Kaspersky Anti-Virus always checks whether your entire computer has been scanned for viruses.

During a full scan, the application scans more objects stored in your computer than it does in the real-time protection mode. Therefore, we recommend that you scan your computer at least once a week, as a preventive measure. The application will remind you when it is the best time to start a full scan. If the main application window is closed, a pop-up window containing a recommendation to start a full scan will appear above the Kaspersky Anti-Virus icon in the system tray (if pop-ups are not disabled, see section 14.9, page 96).

For more detailed information, open the main application window and see the full scan status in the right section of the **Protection** tab (see Figure 5). The full scan status is represented by one of the following icons:

– It is extremely important that you perform a full computer scan now.

– You should perform a full computer scan now. You may also need to restore the recommended settings before you start the scan.

– A full scan is performed on a regular basis or is being performed at the moment.

If required, you can also start a full scan directly from this tab by following the perform a full computer scan hyperlink.

Kaspersky Lab recommends that you schedule a full scan to start automatically (see section 6.4, page 45). The full scan status indicates whether the scheduled scan mode is enabled.

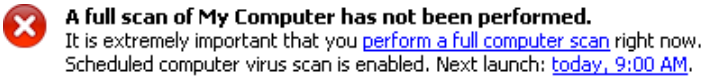
A full scan of My Computer has not been performed.
It is extremely important that you perform a full computer scan right now.
Scheduled computer virus scan is enabled. Next launch: today, 9:00 AM.

Figure 9. Information about the necessity of a full scan

6.2. Scan settings to be used

Kaspersky Anti-Virus starts an on-demand scan using the default settings recommended by Kaspersky Lab (see Chapter 3, page 21). The status of the current scan settings are displayed in the right section of the **Settings** tab of the main application window (see Figure 6) using the following icons:

On-Demand Scan settings do not match the recommended settings.

On-Demand Scan settings match the recommended maximum protection settings.

If necessary, you can change these settings. You can change the protection level and specify the type of action to be performed if a suspicious or infected object is detected.

Note that the protection level and other settings that you assign will APPLY TO ALL types of on-demand scan, including full scans of your computer and scans of selected disks, folders, files, etc.

If you exclude, for example, a particular disk from the scan scope (see section 14.2, page 80) then this disk will not be scanned when you select it for an on-demand scan (see section 6.5, page 46).

To change the protection level and/or type of action to be performed if a dangerous object is detected:

1. Click modify settings in the right section of the **Settings** tab or Configure On-Demand Scan in the left section of the **Settings** tab.
2. In the **Configure On-Demand Scan** window (see Figure 10) that opens after you click the above hyperlink, select the desired *scan level*, which defines the extent of your computer's anti-virus protection. The default level is **Recommended**. You can change it by moving the **Scan level** slider up or down. Below is a discussion of the available protection levels and of situations when the use of a certain protection level is recommended:

   - **Maximum protection** – thorough scan of the entire computer or a particular disk, folder or file.

     We recommend that you use this protection level if you suspect that your computer has been infected with a virus. A detailed discussion of infection symptoms is provided in Chapter 1, page 6.

   - **Recommended** – a scan of the entire computer or a specified object using settings recommended by Kaspersky Lab.

     We recommend that you use this protection level by default as it ensures an optimal combination of scan speed and thoroughness.

   - **High speed** – high-speed anti-virus scan of your computer or of a selected object.

     This protection level ensures scanning at maximum speed due to a reduction in the number of objects to be scanned.

The table below contains a list of all objects that will be scanned at each protection level. The **+** sign indicates that the object will be scanned if the corresponding protection level is selected, while the **–** sign indicates that the object will not be scanned.

	Maximum Protection	**Recommended**	**High Speed**
Area selected by the user	+	+	+[3]
Disk boot sectors, RAM	+	+	+
OLE-objects	+	+	+
Packed files	+	+	+
Self-extracting archives	+	+	+
Objects executed at the operating system startup	+	+	–
Archives	+	+	–
Email databases and messages	+	-	-

For each of the above protection levels, you can specify *exclusions* - a list of objects that will not be scanned (for more details see section 14.4, page 83). However, we recommend that you specify such exclusions only in special cases.

3. Specify the type of action to be performed when a dangerous object is detected during the scan:

- **Prompt user for action once the scan is completed** – suggest processing of dangerous objects detected when the scan is complete. This is a default mode and does not require your constant presence at the desk. Since this scan may take considerable time, we recommend using this mode when you cannot control processing dangerous objects as they are detected.
- **Prompt user for action** – ask user about the action to be performed on detected objects. A list of possible actions will be displayed, one

[3] The virus scan will include potentially infectable objects only.

of which will be recommended by Kaspersky Lab. Select this mode if you are staying at your computer during the scan.

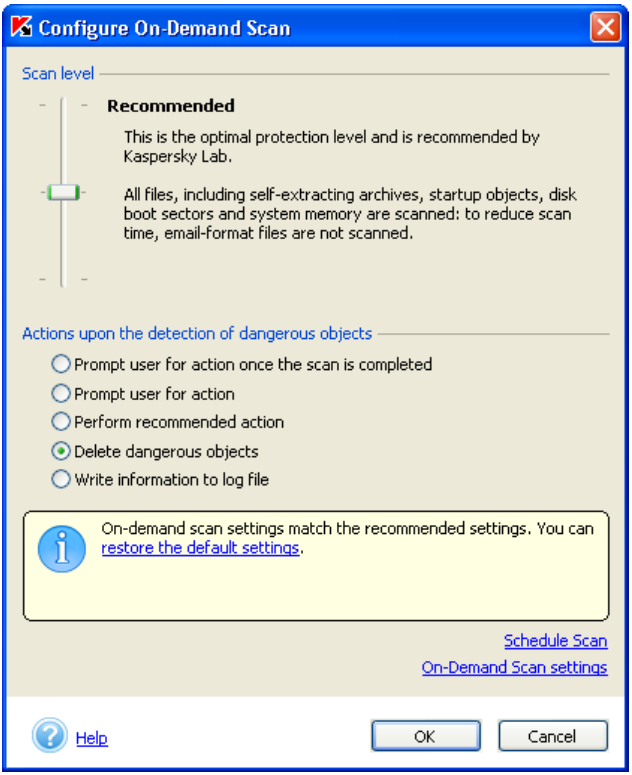
Configure On-Demand Scan
Scan level
Recommended
This is the optimal protection level and is recommended by Kaspersky Lab.
All files, including self-extracting archives, startup objects, disk boot sectors and system memory are scanned: to reduce scan time, email-format files are not scanned.
Actions upon the detection of dangerous objects
Prompt user for action once the scan is completed
Prompt user for action
Perform recommended action
Delete dangerous objects
Write information to log file
On-demand scan settings match the recommended settings. You can restore the default settings.
Schedule Scan
On-Demand Scan settings
Help
OK
Cancel

Figure 10. On-Demand Scan configuration

Perform recommended action – perform the action recommended by Kaspersky Lab. Since the recommended actions are always well justified, you can select this mode in most cases. The recommended actions may be as follows:

- *disinfect* infected objects;
- *quarantine* suspicious or infected objects.

Sometimes, after a file has been quarantined, a message appears notifying the user that the object cannot be deleted. This is related to the fact that quarantined objects are copied to the quarantine folder and deleted from their initial location. However, some objects cannot be deleted this way, as, for example, objects being used by another application.

- *delete* a dangerous object if it could not or cannot be disinfected.

Delete dangerous objects – delete dangerous objects detected during the scan without making an attempt to disinfect them and without asking user's confirmation. A copy of the deleted object will be saved in a Backup. This mode is recommended only if you are certain that you will not lose any valuable information.

Write information to log file – the application will only report infected and suspicious objects found during the scan but will not perform any action on such objects. This mode is not recommended for most cases because all the infected and suspicious objects will remain in your computer.

In some situations no action can be performed on an object, for instance, if an infected object is being used by another program at the time of deletion and therefore cannot be processed. In this case, a message will be displayed (see Figure 11) with a suggestion that you:

- *disinfect at system startup.* This action will be listed only if this object can be disinfected;
- *delete at system startup*;
- *skip* – do not perform any action on the object, only report its detection in the application report.

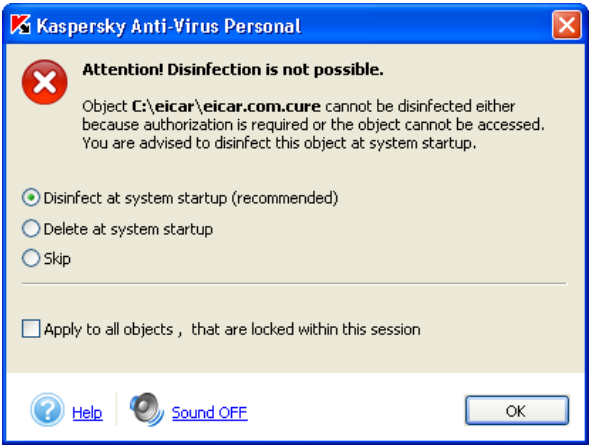
Kaspersky Anti-Virus Personal
Attention! Disinfection is not possible.
Object C:\eicar\eicar.com.cure cannot be disinfected either because authorization is required or the object cannot be accessed. You are advised to disinfect this object at system startup.
Disinfect at system startup (recommended)
Delete at system startup
Skip
Apply to all objects , that are locked within this session
Help
Sound OFF
OK

Figure 11. Immediate disinfection is not possible

For successful treatment (disinfection or deletion) of objects at system startup, the scan procedure during which such objects were detected must be fully completed. If you interrupt the scan procedure, such objects will not be disinfected/deleted.

6.3. Starting an on-demand scan

To start an on-demand anti-virus scan of your entire computer:

click Scan My Computer in the left section of the **Protection** tab (see Figure 5)

After clicking this hyperlink a scan dialog box will open (see Figure 8). This dialog box displays the percentage of scan progress, the name of the object currently scanned, the estimated time of the scan completion and the general statistical data about the objects scanned, disinfected, deleted and quarantined so far.

You can hide the scan window (see Figure 8) by clicking the button in the top right corner or by selecting the **Close this dialog box and resume scan** option in the window that opened.

You can view the scan results in a report (for more details refer to section 14.8, page 91).

6.4. Scheduled full scan

You can schedule a regular full scan of your computer to be performed according to a special schedule. For example, you may choose to schedule the start of a full on-demand scan at lunch time.

To schedule an automatic start of a full scan:

1. Click Configure On-Demand Scan in the left section of the **Settings** tab (see Figure 6).
2. When the **Configure On-Demand Scan** dialog box opens (see Figure 10), click Schedule Scan to open a **Schedule Scan** dialog box.
3. When the **Schedule Scan** dialog box opens (see Figure 12), set up the schedule for this task to be performed as follows:

   Specify scan interval in days – perform an anti-virus scan at a certain interval in days. The default setting is a daily scan at 8 pm. If you wish to modify the default schedule and start time, select the **Every** option and enter the desired scan interval in days in the field beside it. Specify the scan start time in the Scan start field.

   Scan on specific days – specify days on which you wish the scan to be performed. By default the scan is performed weekly, every Friday at 8 pm. If you wish to modify the default schedule, select days in the **Scan parameters** section and specify the scan start time in the **Scan start** field.

   Do not scan – do not perform the scheduled scan. If you select this option, you will have to start a full computer scan manually.

   Request confirmation for scheduled scan – enable notification on launching the scheduled computer scan. If this box is checked, the **Scheduled task launch** window (see Figure 13) will be displayed. Press the **Start** button in order to start the scheduled task. In order to postpone the scan for a certain time, select the required interval in the drop down list and press the **Delay** button. If no action is selected within 3 minutes, the task will be launched automatically.

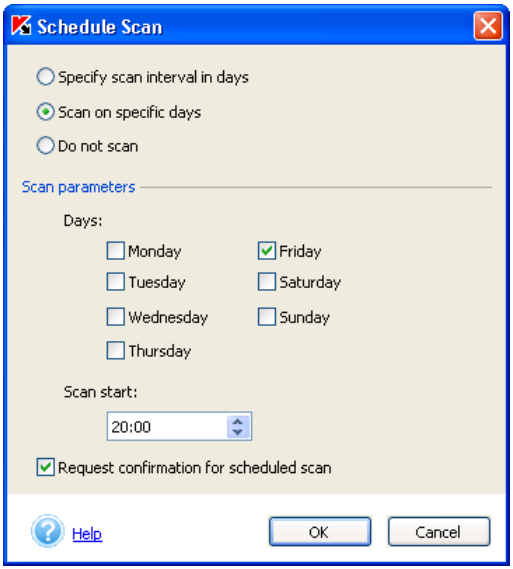

Figure 12. Setting up a scheduled scan

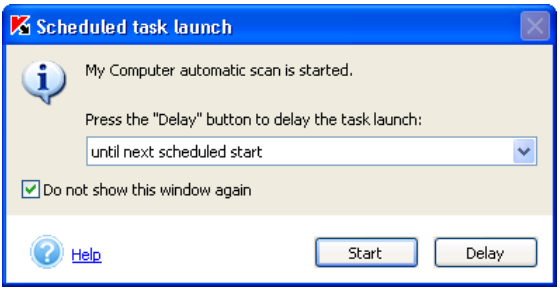

Figure 13. Prompt to run a scheduled task

4. Click the **OK** button.

6.5. On-demand scan of selected objects

Sometimes you need to scan particular objects rather than the entire computer. Such objects may include, for example, a hard drive with program files and games, email databases that you have brought from the office or an archive

attached to an email message that you have received. You can select objects to be scanned using either Kaspersky Anti-Virus or standard Windows tools (for example, **Windows Explorer**, **My Computer**, etc.).

To scan an object selected using standard Windows tools:

select and right-click the object you wish to scan and when the shortcut menu appears, select the **Scan for viruses** command (see Figure 14).

To select and scan objects using Kaspersky Anti-Virus follow the following steps:

To select and scan an object using Kaspersky Anti-Virus Personal:

click Scan objects in the left section of the **Protection** tab (see Figure 5).

The **Select objects to scan** window (see Figure 15) will open; this window contains the list of objects that can be scanned for viruses, and is provided with buttons for editing this list and controlling the scan.

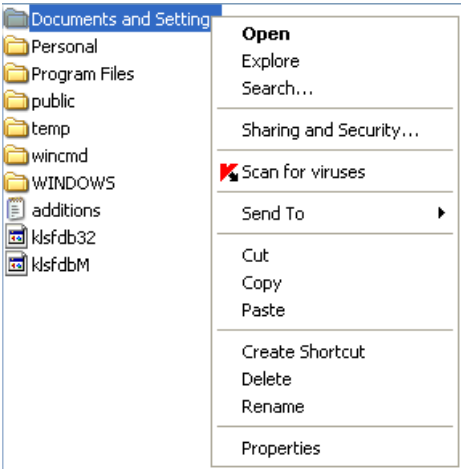

Figure 14. Scanning an object using standard Windows tools

The initial list includes the following objects:

- removable drives, including floppy disks and CD-ROM;
- hard drives;
- Microsoft Outlook and Microsoft Outlook Express mailboxes;
- **My Documents** folder.

- System memory;
- Startup objects;
- Disk boot sectors;

To add a new object to the list, click **Add** and using the file selection window browse to the file or folder you wish to add. All added objects will be available in this list for future scans.

To delete an object from the list, check the corresponding box and click **Delete**. Note, however, that you can delete from the list only those objects that you have added manually. Objects that were included in the initial list cannot be deleted.

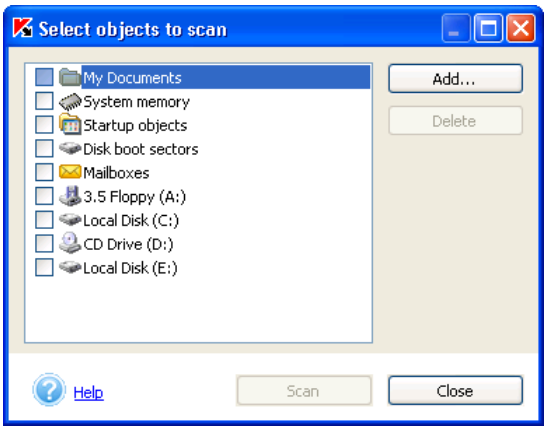

Figure 15. Selecting objects to be scanned

To select and scan objects from the list:

1. Select objects you wish to scan from the list.
2. Click **Scan** to start the scan.

Regardless of how the scan was started (from Kaspersky Anti-Virus or from the Windows shortcut menu), the **Scan** window will appear (see Figure 8). This contains a scan progress bar showing the scan progress, the time the scan started, estimated or actual time of completion of the scan, and the name of the object currently being scanned.

The scan results are documented in a report (see section 14.8, page 91).

6.6. Scanning archives

Kaspersky Anti-Virus scans archives if the **Maximum Protection** or **Recommended** protection level is selected and if these archives have not been previously excluded from the scope of the scan (see section 14.2, page 80).

Kaspersky Anti-Virus Personal scans all objects contained within archives, but disinfects only *zip, arj, cab*, *rar, lha and ice* archives.

Kaspersky Anti-Virus Personal DOES NOT DISINFECT self-extracting archives!

If an archive or an object within an archive is protected with a password and the mode of prompting for the password is enabled, you will be prompted for the password before scanning continues (see Figure 16). If you selected the mode of delayed objects processing (that is if you selected the **Prompt user for action once the scan is completed** action in the scan settings, see section 6.2, page 39), the prompt for the password will be displayed once the scan is complete.

You can enable or disable the prompt for password by checking the ☐ **Do not ask for password when scanning objects** box in the **On-Demand Scan settings** window accessible via **Configure On-Demand Scan** (see section 14.2, page 80).

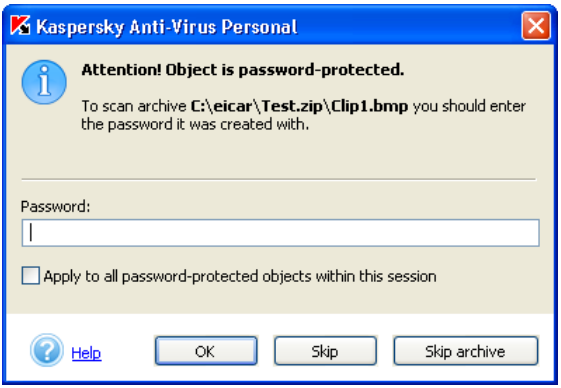

Figure 16. Entering password to scan an archive

In the **Password** field, enter the password required to access this archive or an object within this archive and click **OK**. The archive, and all objects contained within it, will be scanned after the password is entered.

While processing objects within archives, Kaspersky Anti-Virus unpacks an archive to a temporary folder, scans the objects, processes them, packs them into a new archive with the same name and copies this new archive to the initial location of the original archive, thus overwriting the existing original archive. A similar procedure is used for processing password-protected objects within archives. Note that after the objects have been processed, they will be packed into a new archive with no password.

If another password-protected archive is found within the archive being scanned, Kaspersky Anti-Virus tries to apply the password used to access the first (containing) archive to the second (contained) archive. You will only be asked to enter a new password if the password is invalid.

If you do not want to scan a particular password-protected object within an archive, click the **Skip** button and proceed with the scan.

If you do not know the password, the application will be unable to scan this password-protected archive and the objects contained within it. We recommend that you click **Skip** and proceed with the scan.

When you check the **Apply to all password-protected objects within this session** box, the action that you select after checking this box will be applied to all password-protected objects.

For example, if you check this box and click **Skip archive** button, all password-protected archives will be skipped during this scan.

If you enter the password, check the box and click the **OK** button, then this password will be automatically used to access all password-protected objects within all archives in this session. If the password is invalid for a certain object, such object will be skipped.

When an infected object is detected in an archive Kaspersky Anti-Virus will make an attempt to disinfect this object. If disinfection is not possible the object will be deleted from an archive.

If an archive cannot be disinfected and **Perform recommended action** is selected in the on-demand scan settings as an action to perform upon the detection of dangerous object, Kaspersky Anti-Virus will not delete an archive and will only write the information about its detection to report.

If the actions **Prompt user for action once the scan is completed** or **Prompt user for action** are selected in the on-demand scan settings (see section 6.2 on page 39), you will be able to delete the archive that cannot be disinfected by choosing **Delete** action in the window of inquiry of actions upon the detection of a dangerous object (see Figure 21). Besides you can delete the given archive manually.

CHAPTER 7. SCANNING A REMOVABLE DRIVE

Your computer can easily be infected with viruses residing on floppy disks, CDs, and other removable media. If a floppy disk (or a bootable CD) you have used was infected with a boot virus, and you rebooted with the disk left in your drive, this may have gravest consequences to your system.

We recommend that you scan all removable media before using them.

You can scan removable media either from the Kaspersky Anti-Virus main window or using the Windows shortcut menu accessible from **Windows Explorer**, **Desktop**, etc.

To scan removable media for viruses from the Windows shortcut menu:

select and right-click the drive(s) (you can select the CD-ROM and the floppy disk at the same time). When the shortcut menu appears, select **Scan for viruses** (see Figure 14).

To scan a CD-ROM or a floppy disk for viruses from the main application window of Kaspersky Anti-Virus:

1. Insert the disk into the CD-ROM drive or the floppy disk into the floppy drive. Note that the application can scan both the CD and floppy disk at the same time.
2. Click Scan removable drives in the left section of the **Protection** tab (see Figure 5).

or

Using the Scan objects hyperlink, go to the **Select objects to scan** window (see Figure 15), select removable drives and press the **Scan** button.

You can view the scan progress (percentage competed) in the **Scan** window that opens immediately after the scan is started (see Figure 8).

If you select only one removable drive for scanning, Kaspersky Anti-Virus will prompt you to insert the disk into the next removable drive after the scan is completed.

Note the following application's features:

- If the CD or the floppy disk drive is empty or disconnected, the drive will not be scanned. No message will be displayed.
- A CD, floppy disk or other removable medium inserted into its drive after the scan has started will not be scanned.
- If you eject the CD or floppy disk, or disconnect the drive while the scan is in progress, the application will enter error information into the report but no message will be displayed. After this next removable drive, if one exists on your computer, will be scanned.

Each time a new removable drive is connected to the system (i.e. when the drive is detected by the system as new hardware), Kaspersky Anti-Virus will scan such drive for boot-viruses provided that the real-time file protection is enabled.

CHAPTER 8. CONFIGURING REAL-TIME PROTECTION

Real-time protection of your computer means that Kaspersky Anti-Virus constantly monitors all potentially unsafe actions performed on your computer as far as anti-virus and network security are concerned. Such actions include opening or saving files (after you modify them), viewing incoming mail, sending e-mail messages, executing files, executing scripts in Microsoft Internet Explorer, etc. When any of these actions are attempted by the user or by any application installed in your computer, Kaspersky Anti-Virus scans it, and then, depending on the scan results, either permits or prohibits the action or displays a message.

8.1. Checking the protection status

The current real-time protection status is displayed in the right-hand section of the **Protection** tab (see Figure 5) in the main application window.

The real-time protection status is indicated by the following icons:

Real-Time Protection is enabled and the protection settings match the recommended settings.

Real-Time Protection is enabled, but the protection settings do not match the recommended settings.

Anti-virus protection is stopped. This status indicates that the protection of your computer has been temporarily disabled.

Real-Time Protection is not working. In this case we recommend to configure the real-time protection settings (see section 14.1, page 79) and then enable it.

8.2. Specifying application actions and setting the protection level

By default, Kaspersky Anti-Virus is using the recommended settings when operating in the real-time protection mode. It blocks access to all dangerous objects that are being accessed for reading, writing or execution, and displays a message prompting the user for action.

Note that archives and email databases WILL NOT BE SCANNED in the real-time protection mode! An exception is self-extracting archives in which only part responsible for the extraction is scanned (the content of the archive will not be scanned) if the **Maximum Protection** level is selected.

While real-time protection is on, you can select both the level of computer protection and the type of action to be performed if a dangerous object is detected.

To configure application actions upon detection of a dangerous object:

1. Click Configure Real-Time Protection in the left section of the **Settings** tab (see Figure 6) or modify settings in the status area of the **Settings** tab.
2. When the **Configure Real-Time Protection** dialog box opens (see Figure 17), select the protection level using a slider. By changing the protection level, you change the balance between the speed of the scan and the number of objects to be scanned. The fewer objects scanned, the faster the scan will be.

   Kaspersky Anti-Virus allows the user to select one of three protection levels:

   - **Maximum Protection** – this level ensures maximum monitoring of objects that are being opened, saved or run.
   - **Recommended** – this level of protection is recommended by Kaspersky Lab. At this level, the same types of object are scanned as at the **Maximum Protection** level, except for self-extracting archives.
   - **High Speed** – this level ensures good computer performance while you are working with programs that require considerable RAM resources, since the list of objects to be scanned is shorter.

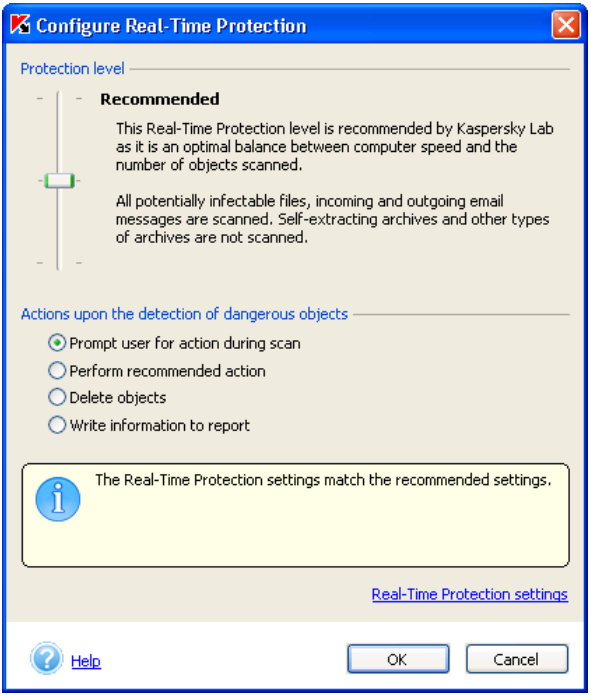
Configure Real-Time Protection
Protection level
Recommended
This Real-Time Protection level is recommended by Kaspersky Lab as it is an optimal balance between computer speed and the number of objects scanned.
All potentially infectable files, incoming and outgoing email messages are scanned. Self-extracting archives and other types of archives are not scanned.
Actions upon the detection of dangerous objects
Prompt user for action during scan
Perform recommended action
Delete objects
Write information to report
The Real-Time Protection settings match the recommended settings.
Real-Time Protection settings
Help
OK
Cancel

Figure 17. Real-time protection configuration

The table below contains a list of all objects that may be subject to an anti-virus scan. The **+** sign indicates that the object will be scanned if the corresponding level is selected, while the **-** sign indicates that the object will not be scanned.

	Maximum Protection	**Recommended**	**High Speed**
Files that potentially can be infected	+	+	+
Disk boot sectors	+	+	+
Packed files	+	+	+

	Maximum Protection	Recommended	High Speed
OLE objects	+	+	+
Data received from the network	+	+	+
Incoming email messages[4]	+	+	+
Outgoing email messages[5]	+	+	–
Self-extracting archives[6]	+	–	–
Email databases and messages	–	–	–

You can specify files to be excluded from the scan scope at each level of real-time protection, or disable real-time protection. For details see section 14.4, page 83.

3. Specify types of action to be performed on detection of a dangerous object:

   Prompt user for action during scan– deny access to the object and display a message prompting the user to choose which action is to be performed on the object. This is the default mode.

   If you do not specify the action within 30 seconds after the message is displayed, the recommended action will be performed on this object. Each type of detected object has its own recommended action. For example, for infected objects the recommended action is *Disinfect*. Text **(recommended)** is always displayed next to the name of the recommended action.

[4] Incoming POP3 mail
[5] Outgoing SMTP mail
[6] Only part of self-extracting archives responsable for the extraction (not the content of the archive) will be scanned.

The list of possible recommended actions is as follows (a subset of these actions is available for each different type of object):

- *disinfect* infected objects;
- *quarantine* suspicious objects that are possibly infected with a virus or a virus modification;

Sometimes, after a file has been quarantined, a message appears notifying the user that the object cannot be deleted. This is related to the fact that quarantined objects are moved: copied to the quarantine folder and deleted from their initial location. However, some objects cannot be deleted this way, as, for example, objects being used by another application.

- *delete* dangerous objects that could not be disinfected;
- *skip* – do not perform any action on objects, but record information on their detection in the report.

Perform recommended action – deny access to the object and perform a recommended action on this object. The recommended action for infected objects is *Disinfect*, for possibly infected objects it is *Quarantine*, and for trojan horses and worms it is *Delete*.

Delete objects – delete objects without any additional warning to the user.

Write information to report – block access to the object, do not display messages prompting user for action.

8.3. Stopping real-time protection

Sometimes you may need to stop real-time protection while using your computer. In order to do this, open the Kaspersky Anti-Virus shortcut menu and select the **Stop Real-Time Protection**.

As disabling anti-virus protection completely is not recommended, Kaspersky Anti-Virus will suggest that you stop temporarily.

Select one of the following options in the **Stopping real-time protection** window (see Figure 18):

- **In 5/10/15 minutes** – the protection will be enabled after the specified period of time.
- **Next time you connect to the network** – the protection will be enabled immediately after your computer connects to the network (this option appears in the list if the computer is currently disconnected from the network).
- **Next time Kaspersky Anti-Virus Personal is started** – protection will be enabled if you start the program from the **Start** → **Programs** → **Kaspersky Anti-Virus Personal** menu or after the system restart (provided that the automatic program start a the system startup mode is enabled).
- **Manually only** – protection will only be enabled if you start it manually.

If necessary, you can also completely disable one of the application components: file system protection, mail protection or protection against network attacks (see section 14.1 on page 79).

Stopping real-time protection
Real-time protection of your computer will be temporarily stopped.
This may result in penetration of viruses into your computer.
Select when you wish to resume real-time protection:
In
5 minutes
Next time Kaspersky Anti-Virus Personal is started
Manually only
Do not show this window again
Help
OK
Cancel

Figure 18. Temporarily disabling anti-virus protection

CHAPTER 9. PROTECTING YOUR COMPUTER AGAINST NETWORK ATTACKS

Kaspersky Anti-Virus Personal 5.0 ensures the protection of your computer against hackers attacks attempted from the local area networks and from the internet.

Hackers attacks are detected using the database of the currently known attacks. This database is updated and installed along with the anti-virus database (details see Chapter 13 page 69).

By default protection against hackers attacks is enabled when the Kaspersky Anti-Virus is started. It scans all data received via the network irrespective of the source of such data (local area network or internet).

If your protection against hackers attacks is disabled, we recommend that you enable it as follows:

1. Follow the Configure Real-Time Protection hyperlink in the left part of the **Settings** tab (see Figure 6) or the modify Real-Time Protection settings hyperlink from the status information area in the **Protection** tab.
2. In the **Configure Real-Time Protection** window (see Figure 17) follow the Real-Time Protection settings hyperlink to access the **Real-Time Protection settings** window and uncheck the ☑ **Disable protection against network attacks** checkbox.

Once an attack on your computer has been attempted, it will be blocked and the corresponding notification (see Figure 19) containing information on the type of the attack, IP address of the attacking computer and the local port (if possible) will be displayed. This notification will not be displayed on the screen if the ☑ **Do not notify about network attacks** box (see Figure 32) is not checked in the settings.

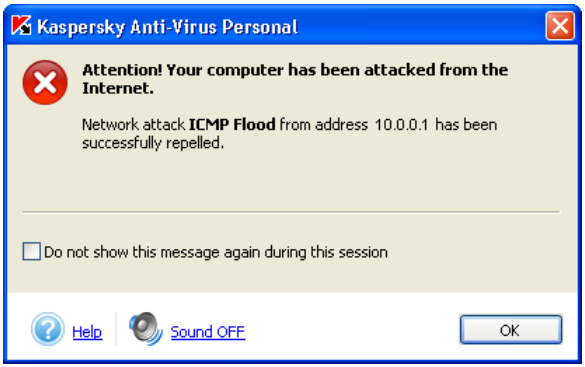
Kaspersky Anti-Virus Personal
Attention! Your computer has been attacked from the Internet.
Network attack ICMP Flood from address 10.0.0.1 has been successfully repelled.
Do not show this message again during this session
Help
Sound OFF
OK

Figure 19. Network attack notification

Details on additional setting of the protection against network attacks see section 14.3 on page 82.

CHAPTER 10. PROTECTING YOUR MAIL FROM VIRUSES

Kaspersky Anti-Virus allows the user to ensure real-time protection of mail received by and sent from your computer. As the email traffic is one of the objects of real-time protection, mail protection is launched at Kaspersky Anti-Virus startup. Any incoming mail message is scanned immediately when it is received and outgoing message – at the moment it is sent. Incoming and outgoing e-mail messages are indicated by the Kaspersky Anti-Virus icon in the system tray: when the message is scanned a blinking image of an envelope appears above the application icon.

Kaspersky Anti-Virus rules for handling email messages are as follows:

- Your email is protected from viruses regardless of which mail client you use [7]. All incoming and outgoing messages are scanned as soon as they are received or when being sent no matter whether you are sending mail using your mail client program or it is being sent by one of the application installed in your computer.
- Upon detection of an infected object in a mail message, a recommended action will be performed on each infected object: Kaspersky Anti-Virus will attempt to disinfect such object and, if disinfection is not possible, delete the object from the mail message.
- If you use mail services of remote web-servers with an Internet browser, for example, with Microsoft Internet Explorer, Kaspersky Anti-Virus will scan attachments when you open them or save them to the disk.

In order to enable anti-virus e-mail protection,

Enable real-time protection (if it is disabled or stopped) and make sure that the ☑ **Disable Real-Time Mail Protection** box in the **Real-Time Protection settings** section is unchecked (see section 14.1, page 79).

The scan of outgoing e-mail messages is controlled by a dedicated box ☑ **Do not scan outgoing mail**.

[7] Kaspersky Anti-Virus Personal provides real-time protection of all incoming POP3 and outgoing SMTP email messages.

To scan Microsoft Outlook or Microsoft Outlook Express mailboxes:

1. Click Scan objects in the left section of the **Protection** tab (see Figure 5).
2. In the **Select objects to scan** dialog box (see Figure 15), check the box **Mailboxes**.
3. Click **Scan**.

As a result, all Microsoft Outlook and Microsoft Outlook Express mail boxes will be scanned.

As a result of processing Microsoft Outlook and Microsoft Outlook Express mail boxes, the date and time of the objects modification will always be changed, irrespective of the action selected to be performed on the object.

Email databases in file format, transferred from another computers, can be scanned on request. By default, upon the detection of an infected email database, Kaspersky Anti-Virus will write the corresponding information to report. Infected email databases can only be deleted manually.

To scan email databases in the format of another email program (for example, The Bat) or databases that you have on disk (for instance, brought home from the office),

1. Use the Scan objects hyperlink in the left section of the **Protection** tab (see Figure 5).
2. In the **Select objects to scan** window that opens (see Figure 15) select a disk or a folder where these databases are stored.
3. Press **Scan**.

CHAPTER 11. DEALING WITH VIRUSES

The actions performed by Kaspersky Anti-Virus upon detection of a dangerous object depend on the real-time protection and on the on-demand scan settings that you have selected. This chapter discusses situations in which Kaspersky Anti-Virus offers a choice of actions to be performed on dangerous objects during the scan or when the scan is complete.

Such situations occur when you select the following actions to be performed on infected or suspicious objects.

- Real-time protection (see Figure 17):
  - **Prompt user for action during scan** In this case the user will be prompted for action immediately when a dangerous object is detected.
- On-demand scan (see Figure 10):
  - **Prompt user for action** The application will offer you to select an action to be performed with a dangerous object when it is detected by Kaspersky Anti-Virus.

  or
  - **Prompt user for action once the scan is completed**. The application offers to select an action to be performed with dangerous objects only if you have initialized processing of these objects - pressed the **Process…** button in the scan results window (see Figure 20).

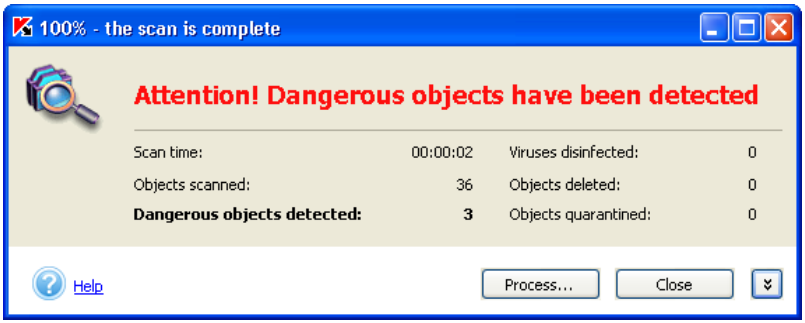

Figure 20. Delayed processing of dangerous objects

When a dangerous object is detected a message will be displayed (see Figure 21), containing:

- a detailed description of the object with an indication of the name of the dangerous program;
- a list of possible actions that you can perform on this object. This list always contains an action recommended by Kaspersky Lab, which is flagged by the word "recommended". Depending on the type of detected object, you may be offered the following actions:
  - **Disinfect (recommended)** – attempt to disinfect the infected object, if treatment is possible.
  - **Delete** – delete the infected or possibly infected object.
  - **Skip** – do not perform any actions; write information on this object into the report.
  - **Quarantine** – quarantine the suspicious object so that later it can be checked, restored, sent to Kaspersky Lab for analysis or deleted (see section 14.4, page 83).
  - **Skip, add to exclusions** – add the detected object to the list of exclusions from anti-virus scan and protection.

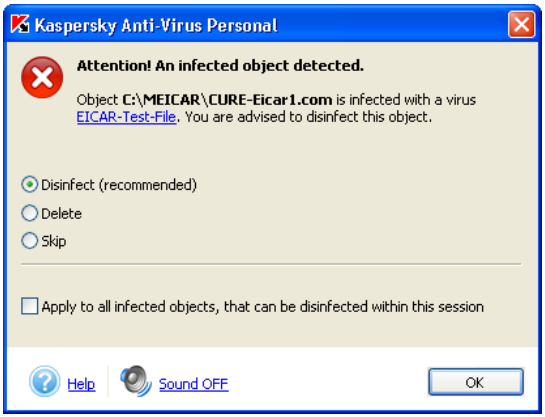
Kaspersky Anti-Virus Personal
Attention! An infected object detected.
Object C:\MEICAR\CURE-Eicar1.com is infected with a virus EICAR-Test-File. You are advised to disinfect this object.
Disinfect (recommended)
Delete
Skip
Apply to all infected objects, that can be disinfected within this session
Help
Sound OFF
OK

Figure 21. A message about the detection of an infected object

You can also apply the selected action to all objects of the same type by checking the corresponding checkbox. Thus, to apply the selected action to all infected objects that can be disinfected, check the **Apply to all infected objects, that can be disinfected within this session** box.

If, for any reason, you decided against processing the objects by selecting the **Skip** option, you can return to their processing later. In order to do this press the process this objects link in the right section of the **Protection** tab. This will open

the **Detected dangerous objects** dialog box (see Figure 22) that contains a detailed description of every dangerous object as well as the link to the corresponding description in the virus encyclopedia at www.viruslist.com.

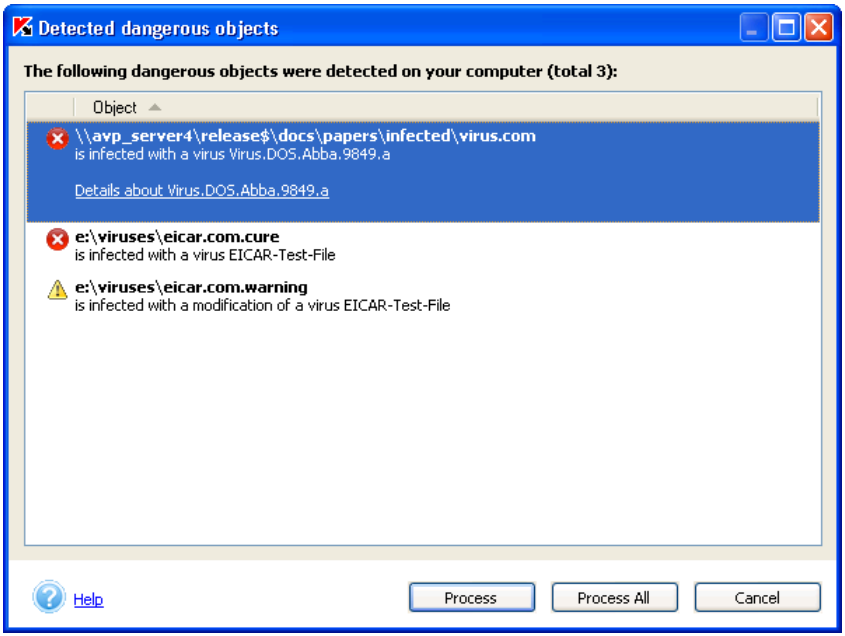

Figure 22. List of detected dangerous objects

You can process the object selected from the list by pressing the **Process** button or launch processing of all objects in the list by pressing the **Process All** button.

In order to delete an object from the list without processing use the **Remove from the list** command from the shortcut menu (see Figure 23).

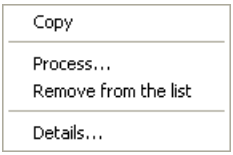

Figure 23. Shortcut menu of the **Detected dangerous objects** window

If any of the dangerous objects has been deleted manually, it will be removed from the list of detected dangerous objects at the time of the attempt to disinfect it.

CHAPTER 12. RENEWING YOUR LICENSE

You can use Kaspersky Anti-Virus Personal only after you have installed the license key included into the distribution kit.

Kaspersky Anti-Virus WILL NOT WORK without the license key!

After the license expires, Kaspersky Anti-Virus retains its functionality except for the anti-virus database and application module update services. You will still be able to scan your computer and email for viruses, and disinfect dangerous objects, but you will only be able to use out-of-date databases that were released on the date of the license expiration. Therefore, we do not guarantee 100% protection from new viruses that appear after your Kaspersky Anti-Virus license expires.

To avoid possible infection of your computer by new viruses, we recommend that you renew your Kaspersky Anti-Virus license.

Kaspersky Anti-Virus will notify you about the license expiration two weeks prior to the expiration date. A reminder message will be displayed each time you start the application during this period.

To renew your license, you must purchase and install a new license key for Kaspersky Anti-Virus Personal. To obtain a new key:

1. Contact the vendor from whom you purchased the product and purchase a new Kaspersky Anti-Virus license key.

or

Purchase a new license key directly from Kaspersky Lab by following the License Renewal hyperlink in the **Support** tab (see Figure 7) or by pressing the **Renew** button on the **Managing License Keys** window (see Figure 24) and filling out the corresponding form in the web page that will open. Upon the receipt of your payment, we will send a new license key to the email address specified in your order.

Kaspersky Lab periodically announces campaigns that allow you to enjoy considerable discounts when you renew you license for the use of our products. In order to keep informed about our offers visit Kaspersky Lab's corporate website and go to **Products → Sales and special offers**.

2. Install the new license key as described below:

   a. Click License Keys in the left section of the **Support** tab (see Figure 7).

   b. In the **Managing License Keys** window (see Figure 24), click the **Add** button.

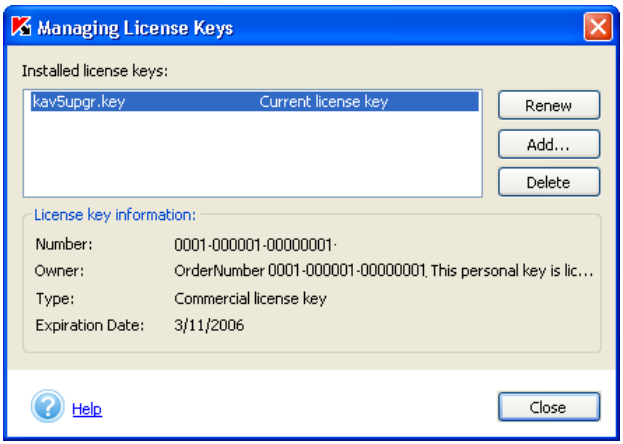

Figure 24. The **Managing License Keys** dialog box

   c. Switch to the folder where the license key (file with extension **.key**) is located. Select the required key and press the **Open** button.

   d. In the window **License Key Activation** that will open, read about the license key you are adding and press the **Activate** button in order to start using this key.

or:

   a. Select the Kaspersky Anti-Virus Personal group in the **Start→Programs** menu and select the **Install license key** item in the group menu.

   b. In the window that will open press the **Browse** button and open the folder in which the license key is located.

   c. Select the required license key file and press the **Open** button.

   d. In the bottom part of the window (see Figure 25) check the box next to the name of the application for which you wish to install the license key. Press the **OK** button.

If the list in the bottom part of the window is empty, the selected license key does not suit any of the Kaspersky Lab's applications installed in your computer.

Select another license key file.

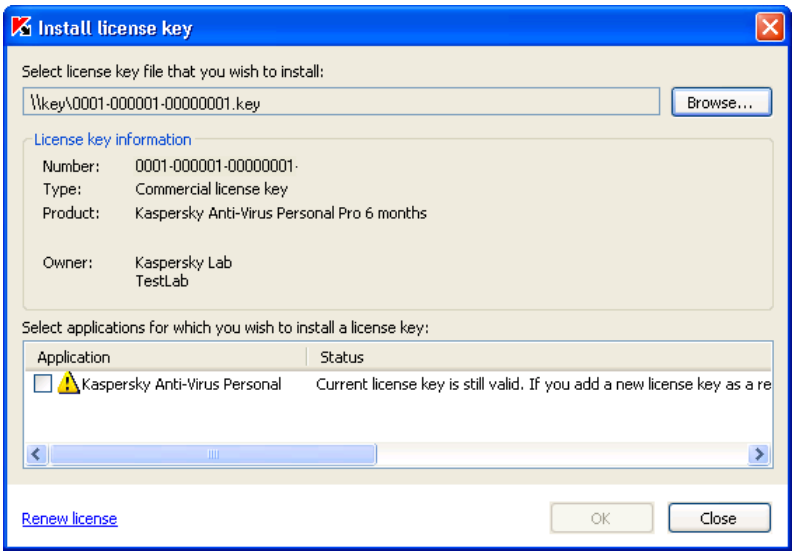

Figure 25. The **License key installation** dialog box

e. Read information about the license key you are adding in the **Key activation** window that will open and press the **Activate button** to start using the key.

CHAPTER 13. DOWNLOADING UPDATES

Kaspersky Lab provides the possibility for its users to update the Kaspersky Anti-Virus Personal application modules, the anti-virus database used by the application to detect malicious software and to disinfect infected objects as well as the network attacks database that is used to protect the user against such attack.

Timely updating of the anti-virus database ensures the safety of your computer. New viruses appear daily, and in response Kaspersky Anti-Virus experts update our anti-virus database with the latest information about these new threats. We recommend that you update your anti-virus database at least once every 3 hours; during periods of virus outbreaks the anti-virus database should be updated as frequently as possible, preferably at least once an hour.

To download updates, Kaspersky Anti-Virus can either connect to the *Kaspersky Lab's updates servers*, or copy the required files from a computer folder, depending on the settings (for details see below).

Updates can be downloaded either on demand, or automatically, by scheduled update. To download updates, your computer must be connected to the Internet. The downloading process is displayed by the special indicator (see Figure 26). If the downloading process is successful, Kaspersky Anti-Virus starts using the new database for scanning the computer.

After the updates have been received and connected, you may need to restart your computer. In this case a corresponding pop-up message will be displayed.

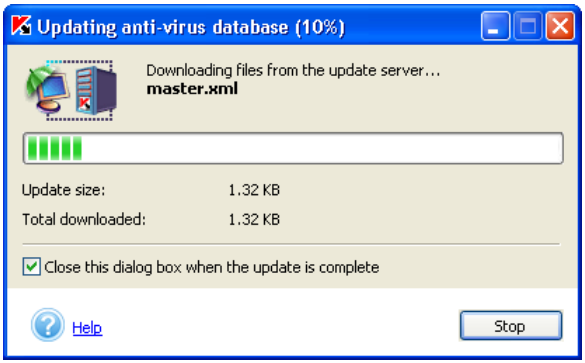

Figure 26. The **Updating** dialog box

13.1. When you should download updates

The application will notify you when your anti-virus database needs updating. You can also check the status of your anti-virus database in the right section of the **Protection** tab (see Figure 5), which will offer advice.

The following symbols are used to reflect the status of the anti-virus database:

– your anti-virus database has been recently updated or is being updated at the moment.

– your anti-virus database must be updated. If updating is impossible because your license has expired, the application offers you information about renewing your license.

– an urgent update is required as the current anti-virus database is extremely outdated, missing or corrupted.

13.2. Which anti-virus database should be used

Kaspersky Anti-Virus offers to use either of two types of anti-virus database with the application:

Standard anti-virus database - the anti-virus database that contains records about all malware known at the moment and about methods used for treating this malware.

If you wish to protect data stored on your computer against potentially dangerous programs, you have to use *Extended anti-virus database*. In addition to records contained in the standard database, this database contains description of adware, spyware hacking tools and other riskware.

The use of standard anti-virus database is sufficient to ensure regular anti-virus protection of your computer. The use of the extended anti-virus database may affect the speed of Kaspersky Anti-Virus operation. Besides, some programs that you use may be treated as riskware.

In order to select the anti-virus database type to be used with your Kaspersky Anti-Virus Personal,

1. Follow the Threats and exclusions hyperlink in the left section of the **Settings** tab (see Figure 6).
2. In the dialog box that will open (see Figure 27) check the **Adware, riskware, automatic dialers** box in the **Detectable threats** section if you wish to use the extended anti-virus database. If you would like to prevent the removal of applications that you use, we recommend that you select an action to be performed with a dangerous object that requires confirmation by the user (see section 6.2 on page 39 and section 8.2 on page 53).

Box **Viruses, worms, trojans, hacking utilities, spyware** is checked by default and cannot be unchecked. It shows that the standard anti-virus database is used for scanning.

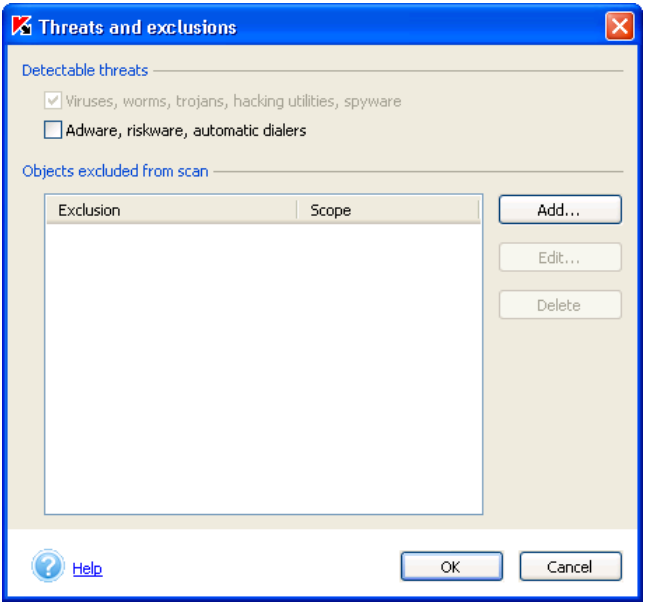

Figure 27. Selecting the type of the anti-virus database

13.3. Downloading updates from the Internet

Kaspersky Lab updates the anti-virus database residing on the update servers every hour.

Kaspersky Lab's updates servers are HTTP and FTP servers where the most recent version of the anti-virus database is kept.

To ensure that your anti-virus database is updated from Kaspersky Lab's update servers, you must apply the settings described in the instructions below:

1. Follow the Configure Updater hyperlink in the left part of the **Settings** tab (see Figure 6).
2. When the **Updater settings** dialog box (see Figure 28) opens, select *from Internet* entry in the **Source of updates** drop-down list:
3. Press **OK**.

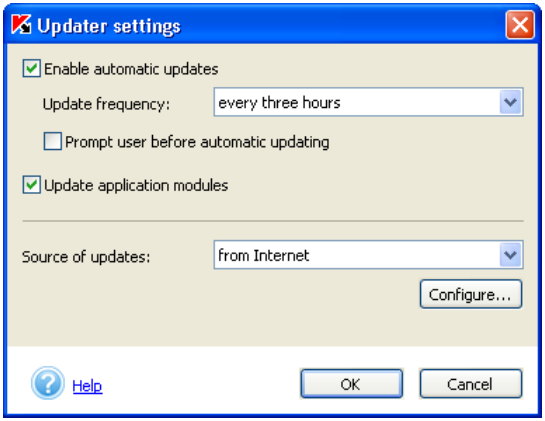

Figure 28. The **Updater settings** dialog box

Your Internet connection settings will be copied from the Microsoft Internet Explorer settings. To view and/or modify these settings, select **Start→Settings→Control Panel→Internet Options→Connections**. If you use a proxy server for your Internet connection, you can configure its parameters. In order to access the proxy server settings press the **Configure…** button (for details see section 13.6 page 75).

13.4. Copying updates from a local folder

If you do not have access to Kaspersky Lab's updates servers (which may be the case if, for instance, you do not have Internet access), you may call our main office on +7 (095) 797-87-00 and get information about Kaspersky Lab partners who can supply you with the anti-virus database, compressed using zip format, on floppy disks or CD-ROMs.

When ordering the anti-virus database, make sure you specify which type of anti-virus database (standard or extended) you wish to receive.

After you receive a zip file with the anti-virus database, you can decompress the database and copy it into any folder of your computer.

To configure anti-virus database updates from a local folder:

1. Click the Configure Updater hyperlink in the left section of the **Settings** tab (see Figure 6).
2. When the **Updater settings** window opens (see Figure 29) select the *from a local folder* option in the **Source of updates** drop-down list.
3. Specify the path to the folder containing the uncompressed zip archive with your anti-virus database, using a standard Windows **Select local folder** dialog box.
4. Press **OK**.

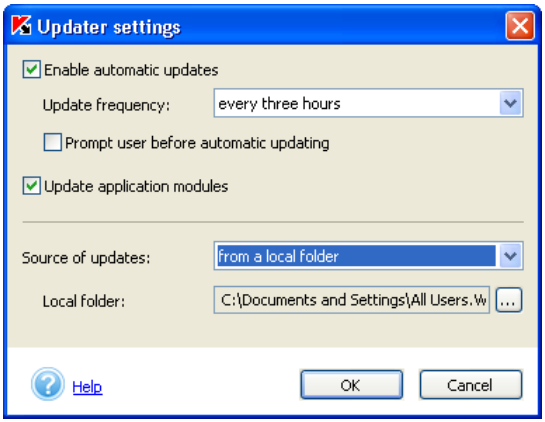

Figure 29. The **Updater settings** dialog box

13.5. Updating Kaspersky Anti-Virus application modules

In addition to the anti-virus database, you can also update Kaspersky Anti-Virus application modules. Application module updates are uploaded to the Kaspersky Lab's update servers from time to time, as such modules are released.

You can update application modules either from the update servers or from a local folder. To do this, check the **Update application modules** box in the **Updater settings** dialog box (see Figure 29).

If you order a zip archive with the updates from Kaspersky Lab or from our partners, make sure to specify that you also would like to receive the application module updates.

During the downloading of the application modules updates a corresponding prompt will be displayed on the screen (see Figure 30). Select one of the following options:

- **Install application modules updates**
- **Do not install application modules update, remind later** – remind the user to install the application modules updates next time Kaspersky Anti-Virus is started.
- **Disable application modules updates installation** – if you select this option the **Update application modules** box in the **Updater settings** dialog box will be unchecked (see Figure 29) and the application modules updating feature will be disabled.

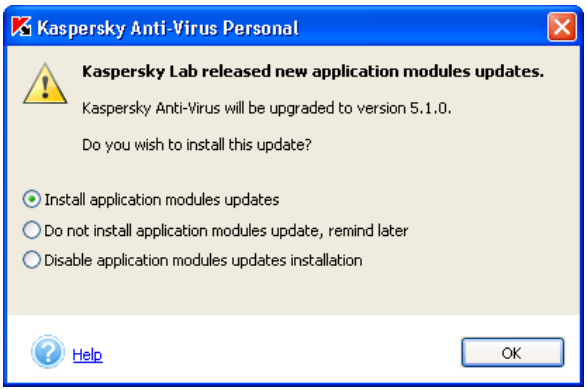
Kaspersky Anti-Virus Personal
Kaspersky Lab released new application modules updates.
Kaspersky Anti-Virus will be upgraded to version 5.1.0.
Do you wish to install this update?
Install application modules updates
Do not install application modules update, remind later
Disable application modules updates installation
Help
OK

Figure 30. Prompt for installation of the application modules update

13.6. Configuring proxy server parameters

By default, Microsoft Internet Explorer internet connection settings will be used for updating the anti-virus database. If you use a proxy server for the internet connection, contact your internet service provide or your system administrator to find out whether you have to specify the proxy server parameters, namely IP address or name, port, authentication parameters, etc.

The proxy server parameters are configured in the **Proxy server settings** dialog window (see Figure 31).

In order to switch to this window, do the following:

1. Follow the Updates hyperlink in the left section of the **Settings** tab (see Figure 6).
2. In the **Updater settings** window that will open (see Figure 29), press the **Configure…** button.

There are two ways to determine the parameters of the proxy server:

- **Automatically detect the proxy server settings**
- **Use a different proxy server**

The first option is selected by default; the proxy server parameters will be copied from Microsoft Internet Explorer.

If your proxy server requires authorization, select the second option and specify the proxy server parameters manually.

Address – IP-address of the proxy server in the format *aaa.bbb.ccc.ddd* or its name.

Port – port number where the proxy server is located. Select one of the values from the dropdown list: *3128*, *8080*, *8082*, *8903* or enter a different value.

If your proxy server requires authorization, check the **Use Authorization** checkbox and specify your username and password in the text fields below as required.

If proxy server authorization is required and you have not specified name and password or if the name and the password entered have not been accepted by the proxy server for some reason, the application will prompt you for the username and the password when the updating process is initiated. If the authorization was successful, the application will use these username and password next time the update is performed. Otherwise you will be asked to re-enter the authorization parameters.

If you have a firewall installed on your server and you cannot connect to the FTP site in the active mode, check the **Use passive FTP mode** box.

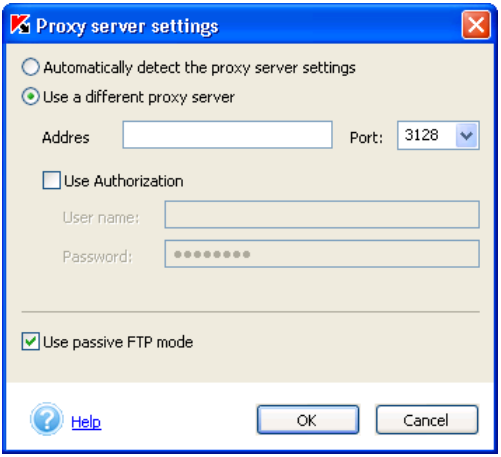

Figure 31. The **Proxy server settings** window

13.7. Updater settings. Scheduled updates

Kaspersky Lab experts recommend that you schedule the application to download updates every three hours; during periods of virus outbreaks the anti-virus database should be updated as frequently as possible.

To schedule updating of your anti-virus database:

1. Click the Configure Updater hyperlink in the left section of the **Settings** tab (see Figure 6).
2. After the **Updater settings** dialog box opens (see Figure 29) check the **Enable automatic updates** box.
3. Select the required updates frequency from the **Update frequency** drop-down list.
4. Check the **Prompt user before automatic updating** box if you would like the application to display the prompt before downloading the anti-virus database (see Figure 13).

If you setup your computer to download updates at a certain interval, for example every 3 hours and it was off for a period of time longer than the specified interval (for example 10 hours), then the anti-virus database will be updated immediately after the computer is turned on next time.

13.8. On-demand updates

To download the anti-virus database updates:

click Update now in the left section of the **Protection** tab (see Figure 5), click the hyperlink in the message, prompting you to update your anti-virus database, in the right section of the window or select the **Update Anti-Virus Database** item from the Kaspersky Anti-Virus shortcut menu.

On-demand or scheduled downloading can only be initiated if your computer is connected to the Internet. If an Internet connection is unavailable, the updating process will not start.

CHAPTER 14. ADDITIONAL SETTINGS

Kaspersky Anti-Virus offers the user the following capabilities to configure and operate the product, namely:

- Configuring the settings of real-time protection and full computer scan.
- Managing quarantined objects.
- Managing backup copies of objects.
- Application performance report analysis.
- Creating a list of exclusions.
- Additional settings.
- Managing Kaspersky Anti-Virus profiles

This chapter contains a detailed discussion of each of the above options.

14.1. Configuring real-time protection settings

By default real-time protection of your computer uses the settings recommended by Kaspersky Lab, but you have a high degree of control over the settings. In addition to the ability to modify the major settings of real-time protection (see Chapter 8, page 53), you may exclude a certain group of objects from the scope of real-time protection, and either partially deactivate or completely disable real-time protection. Such exclusions allow you to decrease the total number of files scanned during real-time protection. For example, you can exclude email messages or scenarios (script files) from scanning, and limit the maximum scan time for an object in seconds.

Additional settings apply for all real-time protection levels (**Maximum Protection**, **Recommended**, and **High Speed**).

These real-time protection settings can be accessed from the **Real-Time Protection settings** dialog box (see Figure 32). You can open this dialog box by clicking Real-Time Protection settings in the **Real-Time Protection Settings** dialog box (see Figure 17).

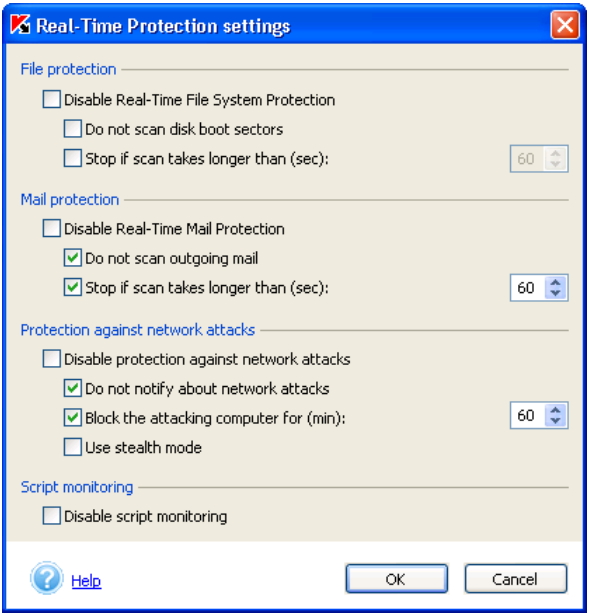

Figure 32. Configuring real-time protection

Kaspersky Anti-Virus allows you to re-apply the default (recommended) settings at any time, thus discarding the customized settings.

To restore the default real-time protection settings for any real-time protection level, click the restore the default settings hyperlink in the right part of the **Settings** tab in the comments to the real-time protection status (see Figure 33) or using the profiles management function (see section 14.11, page 102).

Maximum Real-Time Protection settings are in use.
Upon virus detection, block access and prompt user for action.
Protection level: Maximum Protection.
You can modify settings or restore the default settings.

Figure 33. Information on real-time protection status

14.2. Configuring on-demand scan settings

By default, during a full computer scan, Kaspersky Anti-Virus Personal scans all objects stored on your hard drive (see Chapter 3, page 21) using settings recommended by Kaspersky Lab.

In addition to selecting the anti-virus protection level and customizing the types of action to be performed upon the detection of infected or suspicious objects (see section 8.2, page 53), you can, as with real-time protection, configure additional scan settings for all levels that reduce the number of objects to be scanned.

Additional scan settings can be configured the same way for all scan levels (**Maximum Protection, Recommended** and **High Speed**).

Additional scan settings can be accessed from the **On-Demand Scan settings** dialog box (see Figure 34). You can open this dialog box by clicking the On-Demand Scan settings hyperlink in the **Configure On-Demand Scan** dialog box (see Figure 10).

Here you can exclude certain types of objects from the scan scope. In order to do it check the corresponding boxes

Kaspersky Anti-Virus also allows returning to the recommended setting and rejecting the settings you have configured at any moment while you are using the application.

To restore the settings recommended for any level, click restore default settings in the right section of the **Settings** tab (see Figure 6) or in the comments on the real-time protection status in the **Protection** tab.

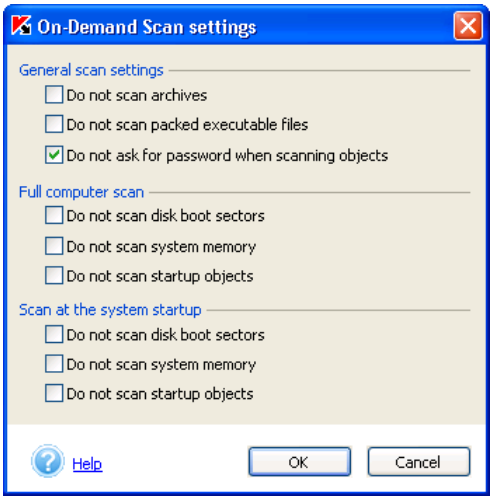
On-Demand Scan settings
General scan settings
Do not scan archives
Do not scan packed executable files
Do not ask for password when scanning objects
Full computer scan
Do not scan disk boot sectors
Do not scan system memory
Do not scan startup objects
Scan at the system startup
Do not scan disk boot sectors
Do not scan system memory
Do not scan startup objects
Help
OK
Cancel

Figure 34. Exclusions from the scope of on-demand scan

14.3. Configuring protection against network attacks

Protection against network attacks can be configured in the **Real-Time Protection settings** dialog window (see Figure 32).

When you enable/disable the real-time protection using the Anti-Virus shortcut menu in the system tray, the protection against network attacks will also be enabled or disabled as the case may be (see 8.3, page 57).

If you wish to disable the protection against network attacks only, without disabling file and mail protection functions, check the ☑ **Disable protection against network attacks** box in the **Real-Time Protection settings** window. After you enable or disable protection, you will have to restart your computer for the changes you have made to take effect.

Additionally, you can configure additional settings as follows:

- **Notifications about network attacks**. By default the program informs the user each time an attack is attempted at the computer. A message will be displayed (see Figure 19) containing information about the type of the attack, the IP address of the attacking computer and the local port (if it is possible to determine it). Since this notification is provided only for reference, you can disable its display by checking the ☑ **Do not notify about network attacks** (in this case, the information about attacks will still be registered in the report).

- **Blocking the attacking computer**. Kaspersky Anti-Virus can block all computers that attempt to attack your computer. By default the function of blocking the attacking computer is disabled. If you decide to enable this function, the default blocking time is 60 minutes. During this time, the any packets sent from the attacking computer to your computer will be blocked. In order to change the blocking period, specify the desired value in the **Block the attacking computer for (min)** parameter. In order to disable the blocking mode, uncheck the checkbox beside this parameter.

- **Stealth mode**. This mode allows only those network activities that have been initiated by the user or by programs installed on the user's computer; all other actions (remote connection to your computer, etc.) will not be allowed. This means that your computer becomes virtually "invisible" for other computers. Besides, the stealth mode allows to prevent any types of DoS (Denial of Service) attacks. At the same time, the stealth mode does not have any negative impact on your internet activities as Kaspersky Anti-Virus allows any network activities initiated by the user.

Attention! Stealth mode does not protect your computer from the harmful actions of trojan programs!

By default the stealth mode is disabled. In order to enable it, check the **Use stealth mode** checkbox.

14.4. Creating a list of exclusions

If you want to exclude some objects from the scope of scan or protection, you can specify a path to such objects or their mask (for example *.bmp) in **Threats and exclusions** window (see Figure 27).

In order to open this window, follow the Threats and exclusions hyperlink in the left part of the **Settings** tab (see Figure 6). The list of exclusions is created using the corresponding buttons.

*In order to add an exclusion, press the **Add** button.*

This will open the **Excluded object** window (see Figure 35) where you can specify the exclusion.

The following types of objects can be specified as exclusions:

- *Disks*, *folders*, *files*, *file masks*.
- *Threats* – types of malicious or potentially dangerous software.
- *Files associated with certain types of threats* – files that are assigned certain types of threats.

In order to exclude a certain folder or files (using file mask) from the scope of Kaspersky Anti-Virus protection,

Fill in the **Object** field using the ... button.

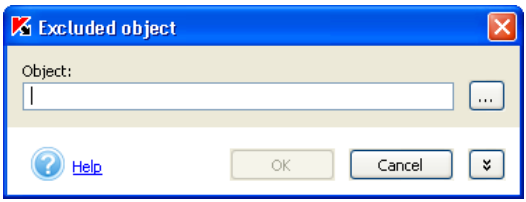

Figure 35. Specifying an exclusion

Listed below are examples of allowed exclusion masks:

- Masks used without specifying the path to objects:
  - ***.exe** – all files with extension exe
  - ***.ex?** – all files with extension ex?
  - **test** – all files with filename test
- Masks used with absolute paths to objects:
  - **C:\dir*.*** – all files in folder C:\dir\
  - **C:\dir*.exe** – all files with extension exe in folder C:\dir\
  - **C:\dir*.ex?** – all files with extension ex? in folder C:\dir\
  - **C:\dir\test** – file C:\dir\test only
  - **C:\dir** – all files in folder C:\dir\ including all subfolders
- Masks used with relative paths to objects:
  - **dir*.*** – all files in all folders under dir\
  - **dir\test** – all files with filename test in folders under dir\
  - **dir*.exe** – all files with extension exe in all folders under dir\
  - **dir*.ex?** – all files with extension ex? in all folders under dir\
  - **dir** – all files in all folders under dir\ and in all their subfolders

We do not recommend to enter ***.*** and * masks as these masks are equivalent to disabling the real-time protection.

We do not recommend selecting as exclusion a virtual drive created based on the file system folder using the *subst* command. This does not make sense as when performing a scan, Kaspersky Anti-Virus will treat this virtual drive as a folder and, therefore, will scan it.

In order to exclude from the anti-virus processing scope all files that were assigned a certain threat type as a result of an anti-virus scan,

open the additional part of the window (see Figure 36) by pressing button and select the threat type in the **The list of detectable threats** dialog box (see Figure 37) that opens by clicking button .

In this window you can search for a threat by a part of its name, sort the list of threats by clicking the heading of the **Name** column and copy the name of a threat into the buffer using the corresponding command of the shortcut menu. You can also view the detailed description of a threat at www.viruslist.com. In order to do it, select the threat in the list and use the **Details** command of the shortcut menu.

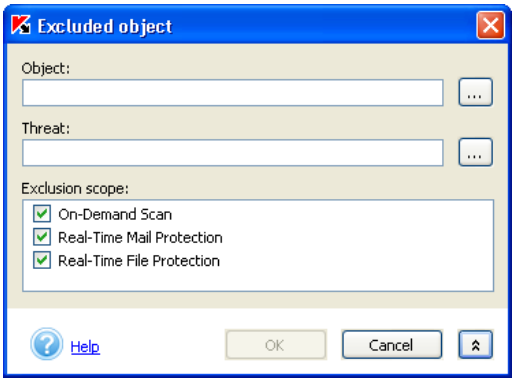

Figure 36. Creating the list of exclusions

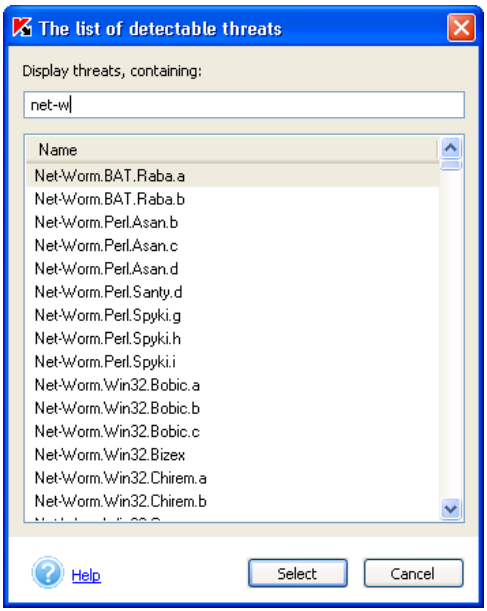

Figure 37. The list of detectable threats

In order to exclude a certain object with a known threat type from the scan scope,

1. Specify the object's name in the **Object** field
2. Enter the threat type in the **Threat** field.

You can also exclude file with a certain threat type using a notification that opens when Kaspersky Anti-Virus has detected such file (see Figure 38).

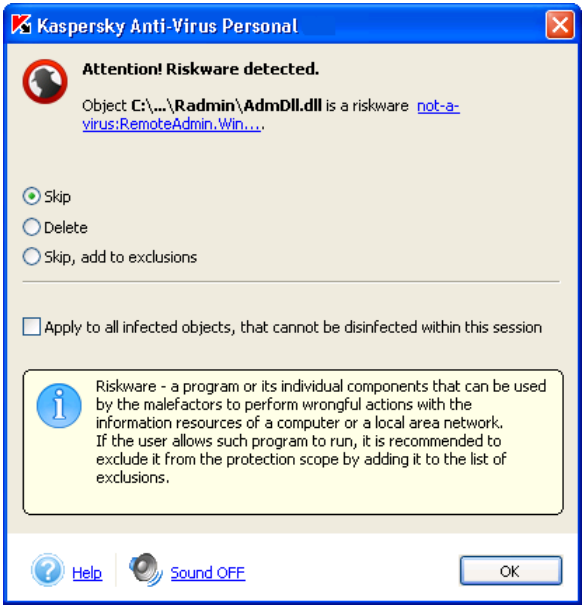
Kaspersky Anti-Virus Personal
Attention! Riskware detected.
Object C:\...\Radmin\AdmDll.dll is a riskware not-a-virus:RemoteAdmin.Win....
Skip
Delete
Skip, add to exclusions
Apply to all infected objects, that cannot be disinfected within this session
Riskware - a program or its individual components that can be used by the malefactors to perform wrongful actions with the information resources of a computer or a local area network. If the user allows such program to run, it is recommended to exclude it from the protection scope by adding it to the list of exclusions.
Help
Sound OFF
OK

Figure 38. Threat notification

Here you can also define the action for which Kaspersky Anti-Virus will use this exclusion. The following actions will be suggested as options:

- **On-Demand Scan** – the exclusion will be used when a full computer anti-virus scan is performed.
- **Real-Time Mail Protection** – the specified exclusion will not be processed by Kaspersky Anti-Virus when found in e-mail message.
- **Real-Time File Protection** – the specified object will not be scanned by Kaspersky Anti-Virus when this object is being opened, run or saved.

14.5. Managing quarantined objects

During the scan of the entire computer, disks or files or when the real-time protection is enabled, Kaspersky Anti-Virus places all objects that are possibly detected with viruses or their modifications into the quarantine folder where you can proceed working with them (rescan, restore, delete, etc.). The quarantined files are stored in a special format and do not impose any threat.

A heuristic code analyzer, detecting up to 92% of new viruses, determines whether a file is suspicious in terms of possible presence of a virus. This mechanism is quite effective and cases of false positives are extremely rare.

We recommend that you update the anti-virus database before scanning quarantined files. The update may contain information about any viruses which have infected the quarantined files, and you may be able to repair the files.

You can manage possibly infected files in the **Quarantine** window (see Figure 39), which can be opened by clicking View Quarantine in the **Protection** tab (see Figure 5) of the main application window or by clicking the View Quarantine hyperlink in the **Scan** window (see Figure 8).

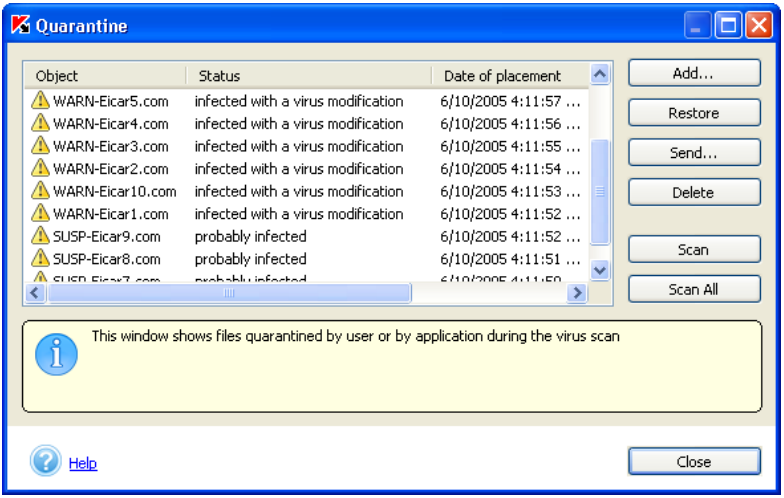

Figure 39. Quarantine for suspicious files

The following actions can be performed from the **Quarantine** window:

- Quarantine a file suspected of being infected with a virus that is not detected by Kaspersky Anti-Virus. To quarantine a file, click **Add** and select the suspicious file in the standard file selection window. The file will be added to the list with the *quarantined by user* status.

- Scan and disinfect all of, or a subset of, the suspicious files using the current anti-virus database. To do this, either click **Scan All**, or select the files to be scanned and click **Scan**.

  After the scanning and disinfection of a quarantined object its status may change to *infected, false alarm*, *not infected,* etc. In this case, a message will give recommendations on how to treat this file.

  The *infected* status means that the object was identified as dangerous but its disinfection failed. We recommend that you delete such objects.

  All objects with the *false alarm* status may be safely restored, as their previous *possibly infected* status was not confirmed by Kaspersky Anti-Virus.

- Restore files from the quarantine folder to their original folders. To restore an object, select it in the list and click the Restore button. When restoring objects quarantined from archives, email databases and mail format files, you must specify the folder to which they are to be restored.

  We recommend that you restore only objects with a *false alarm, not infected* or *disinfected* status because restoring other objects may infect your computer!

- Send suspicious objects to Kaspersky Lab for analysis. We recommend that you only send objects that have retained their possibly infected status after numerous attempts to scan and disinfect them. To send a file to Kaspersky Lab, click Send (for details see Chapter 15, page 104).

  Note that files that you send to Kaspersky Lab for analysis should be scanned by Kaspersky Anti-Virus, using an anti-virus database updated at most one day before you send the file.

- Delete a quarantined object or a selected group of objects. Delete only files that cannot be disinfected. To delete such files, select them in the list and click the **Delete** button.

14.6. Managing backup copies of objects

Backup storage is a special storage area used to store backup copies of objects. Backup copies are created when an object is attempted to be disinfected or deleted for the first time. The major function of the backup storage - to keep these copies so that the initial object can be restored at any moment.

You can manage backup copies via a dialog window **Backup Storage** (see Figure 40). In order to access this window, follow the Backup Storage hyperlink in the left section of the Protection tab (see Figure 5).

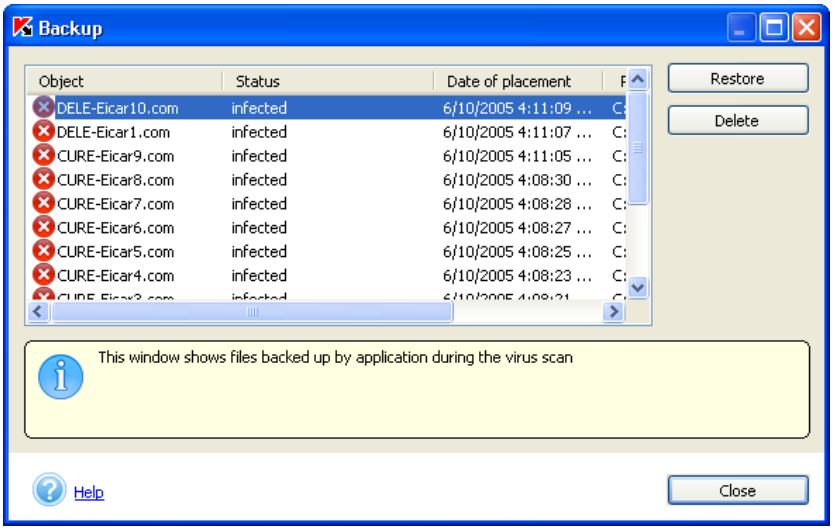

Figure 40. Backup storage

The central part of the window contains the list of backup copies. The following information is provided for each copy: name of the object for which the copy is created, object status, copy creation date and the full path to the initial object's location.

You can restore or delete a copy or several selected copies using the corresponding buttons to the right of the list.

Object is restored from the backup copy under the same name it had before processing.

If an object with the same name is found at the initial location (this is possible if you are restoring an object that was backed up and then disinfected), the corresponding warning will be displayed. You may select a different location for the object being restored or rename the object.

When is it safe to restore backup copies?

When disinfecting objects, their integrity sometimes can not be maintained. If the disinfected file contained important information that have become completely or partly unavailable, you can try to restore the initial object from the backup copy. We recommend that you scan such objects for viruses immediately after their restoration as such object may be successfully disinfected without data loss using updated anti-virus database.

We do not recommend to restore objects from backup copies, if it is not necessary as this may result in an infection of your computer.

By default the period of storing such backup copies and the maximum size of the backup storage are not limited. We recommend that you periodically view and clean the backup storage. You may also setup the program so that it automatically removes older copies and notifies you about the backup storage overflow (for details see section 14.7 page 90)

14.7. Additional quarantine and backup storage settings

You can customize the settings for the creation and operation of the quarantine and of the backup storage. To configure the quarantine settings, click Configure Quarantine & Backup on the **Settings** tab (see Figure 6) of the main application window. Edit the following settings (see Figure 41) in the corresponding section (quarantine or backup storage) of window that will open:

- **Automatically scan quarantined objects every time the anti-virus database is updated**. This mode of Kaspersky Anti-Virus provides for an automatic scan of the quarantined objects each time the anti-virus database gets updated.

  Kaspersky Anti-Virus will not be able to scan quarantined objects immediately after you updated your anti-virus database if you were working with the quarantine at the time of update.

- **Quarantine maximum size ... MB**. By default, the quarantine size is not limited. If you wish to restrict the total size of the quarantined files, check the corresponding box and specify the size using the up and down arrows of the corresponding spin-button box (the default value is 100 MB). If the quarantine size is exceeded, the application will notify you with a message.

- **Delete objects stored longer than ... days**. By default, the storage time of quarantined files is not limited. You can limit this period by checking the corresponding box and specifying the number of days in the corresponding spin-button box (the default value is 90 days).

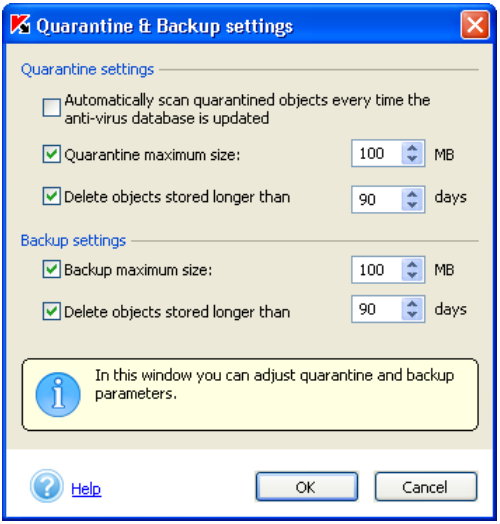

Figure 41. Quarantine and backup settings

The maximum size of the backup storage and the period of time for which the backup copies are stored are similar to the corresponding settings of the quarantine.

14.8. Managing reports

The application maintains reports during anti-virus scans, while the anti-virus database is being updated and while real-time protection is enabled. The reports include information about the objects scanned, processing results and general statistical data.

A complete list of all reports about tasks performed or being performed by Kaspersky Anti-Virus can be viewed in the **Reports** windows (see Figure 42). You can open this window by clicking the Reports hyperlink in the left section of the **Protection** tab (see Figure 5).

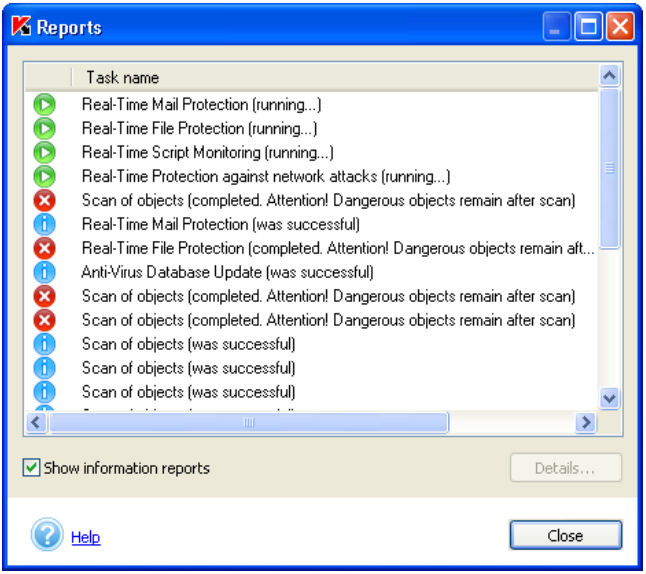
Reports
Task name
Real-Time Mail Protection (running...)
Real-Time File Protection (running...)
Real-Time Script Monitoring (running...)
Real-Time Protection against network attacks (running...)
Scan of objects (completed. Attention! Dangerous objects remain after scan)
Real-Time Mail Protection (was successful)
Real-Time File Protection (completed. Attention! Dangerous objects remain aft...
Anti-Virus Database Update (was successful)
Scan of objects (completed. Attention! Dangerous objects remain after scan)
Scan of objects (completed. Attention! Dangerous objects remain after scan)
Scan of objects (was successful)
Scan of objects (was successful)
Scan of objects (was successful)
Show information reports
Details...
Help
Close

Figure 42. Reports

The following report types are provided:

- or – *Information reports* contain reference information (for example, the task started, the task completed, the task is in progress, the task is paused).
- – *"Attention" reports* contain critical information (for example, Attention! Untreated objects remain).
- – *"Note" reports* comment on important issues of the application's operation (for example, the task was interrupted).

As a rule, information reports are provided for reference only and are of no special interest. The display of information messages can be disabled by unchecking the **Show information reports** box. Note that reports about tasks currently in progress, indicated by icon , will always be displayed.

Reports can be sorted by report type, by title (in alphabetical order) and by task completion time. To sort the reports by any of the above columns, simply click the header of the corresponding column.

To view the settings, statistics and outcome of a specific task listed in the log, select the task and click the **Details** button, or double-click the task.

This will open a new window with a detailed report on the task in the **Statistics**, **Report**, and **Settings** tabs.

During a full scan, you can monitor the task performance the same way (see Figure 8).

For scanning tasks, the **Statistics** tab (see Figure 43) displays general information about the task performed by Kaspersky Anti-Virus, including: the date and time the task was started, the total number of files scanned and the number of infected, disinfected and quarantined objects. For the update task this tab will display the total size of the update files at the source (Kaspersky Lab's update servers or local folder) and the total size of files downloaded to your computer.

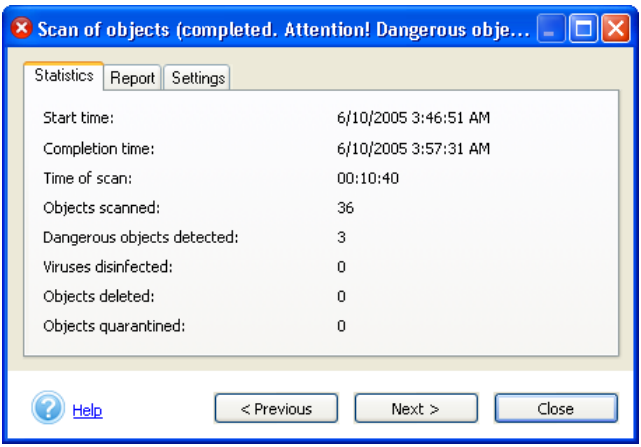

Figure 43. The **Statistics** tab

For scanning tasks, the **Report** tab (see Figure 44) by default only displays information about viruses detected. To display information about files that are not infected as well, check the **Log all reports** box in the **Additional Settings** window of Kaspersky Anti-Virus (see section 14.9, page 96). If you do so, the **Report** tab will contain information on each scanned object. For the update task this tab displays information on each step: on establishing connection with the update servers, about the downloaded files, and installation information. For the update task this information will always be displayed irrespective of whether or not the **Log all reports** box in the **Additional Settings** window is checked.

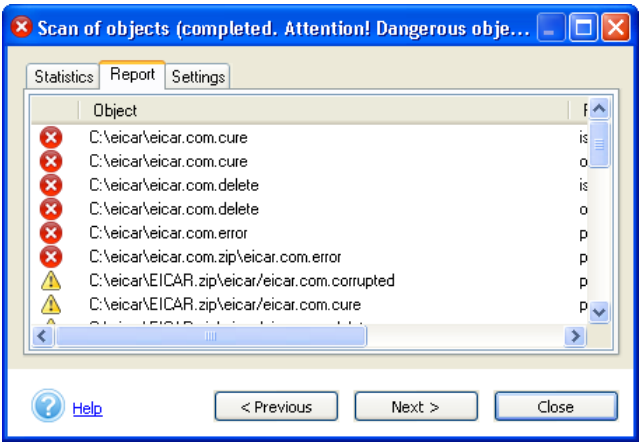

Figure 44. The **Report** tab

For scanning tasks, the **Settings** tab (see Figure 45) displays settings used by the task including the scope of the scan, the protection level set for these tasks and the types of action to be performed on suspicious and infected objects.

This information also includes the list of exclusions from the scan scope if such exclusions have been specified. For update tasks the update type and update source are displayed.

You can select the tasks to be viewed in the **Reports** windows or in the detailed task report dialog box using the **Next >** and the **< Previous** buttons.

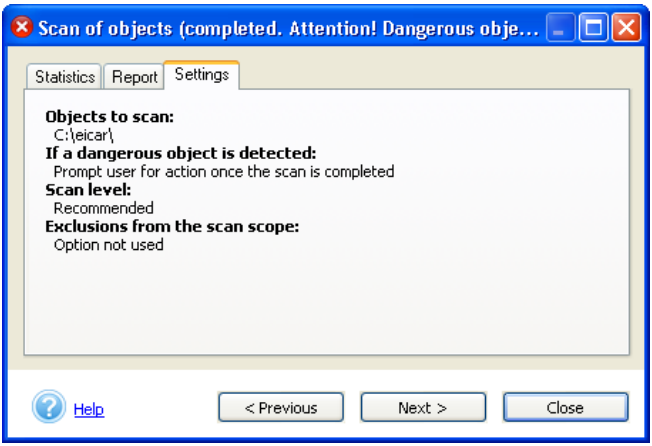

Figure 45. The **Settings** tab

14.8.1 Displaying reports

Kaspersky Anti-Virus allows you to choose which information will be displayed in reports. You may configure the application so that only important information will be recorded in reports, while information and other reference messages will not be entered.

You can enable logging all reports by checking the **Log all reports** in the **Additional Settings** window (see section 14.9, page 96). You may view all messages displayed for instance when you start a full computer scan in the Scan window (see Figure 8) in the **Report** tab.

If this box is checked, a detailed report about the task performed will be compiled, including information about the correct processing of the object.

If the box is unchecked, only “attention” reports and “note” reports will be displayed: for example a message that an object has not been scanned due to an error. Messages about successful processing will not be displayed.

To disable displaying information reports within the current session without unchecking the ***Log all reports*** *box,*

right-click the window while viewing reports in the **Report** tab to open a shortcut menu (see Figure 46) and uncheck the **Show detailed report** flag.

Figure 46. Shortcut menu - **Report** tab

If the **Log all reports** box in the **Additional Settings** window is unchecked, the **Show detailed report** option in the context menu will also be unchecked and disabled and you will not be able to configure displaying information reports.

When you are viewing the report in the monitoring mode (i.e. during the scan in the **Report** tab), by default you will always see the last record of the report. To disable this mode, right-click to open shortcut menu and uncheck the **Show last record of the report** box or simply select a record in the report.

You can also copy information about an individual event into the buffer. In order to do it, select the required event and use the **Copy to clipboard** command from the shortcut menu.

14.8.2 Exporting and sending reports

Kaspersky Anti-Virus allows you to edit the list of reports created based on the results of various tasks. You may access available editing options from the context menu (see Figure 47), which you can open by right-clicking the **Report** window (see Figure 42).

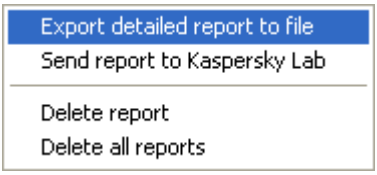

Figure 47. Shortcut used for managing reports

You cannot delete a report while the task creating the report is in progress.

Exporting a detailed report to a file allows you to view its contents in the form of a Microsoft Excel table or a plain text file.

If any task (for instance, a computer scan or anti-virus database updating process) is interrupted or results in an error and you do not know what caused this application behavior, you may send a report on the task to Kaspersky Lab.

To do this, select the report you wish to send in the **Reports** window, right-click the selected report and choose the **Send report to Kaspersky Lab** option in the shortcut menu. This will open a new window of your default email client application (for example, Microsoft Outlook Express) containing a new email message with the report file attached to it. Send this message and Kaspersky Lab will respond to it as soon as possible.

Mail messages are automatically created using exclusively Microsoft Outlook or Microsoft Outlook Express. If you have a different mail program installed on your computer (for instance, TheBat!), you will have to configure your mail program's Simple MAPI to ensure that automatic message creation is supported.

14.9. Additional settings of Kaspersky Anti-Virus Personal

In addition to configuring the settings for particular tasks, Kaspersky Anti-Virus Personal allows configuration of general and service settings (see Figure 49).

In order to configure additional Kaspersky Anti-Virus settings,

Follow the Additional Settings hyperlink in the left part of the **Settings** tab (see Figure 6). This will open a dialog box containing the **General**, **Efficiency** and **Security** tabs.

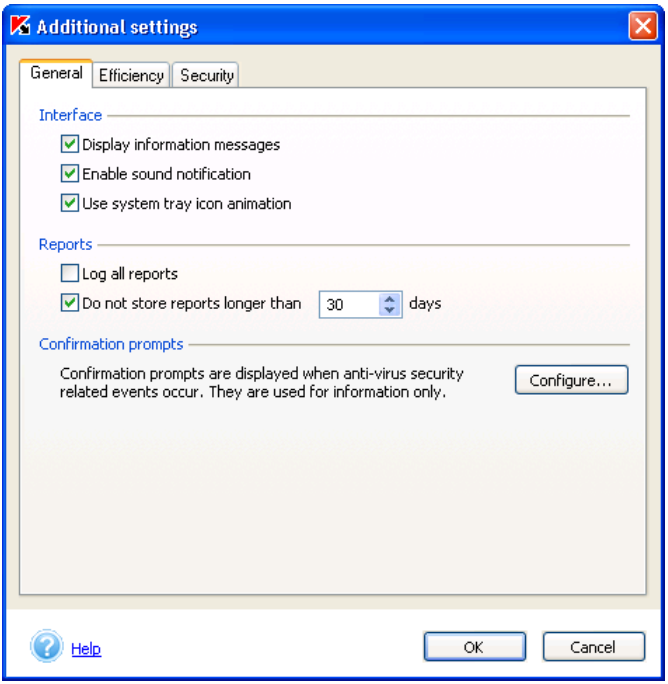

Figure 48. Additional Kaspersky Anti-Virus Personal settings. The **General** tab

Using the **General** tab (see Figure 48) you can configure the following settings:

- **Display information messages** – enable the display of all pop-up tips accompanying the operation of Kaspersky Anti-Virus. We recommend that you do not disable this mode because the application often operates in interactive mode requiring the user's feedback when processing objects.

  Microsoft Windows 98 and Microsoft Windows NT Workstation 4.0 operating systems do not support displaying of informational messages.

- **Enable sound notification** – enable sound effects accompanying some events occurring displayed during Kaspersky Anti-Virus operation. You can view the list of events or modify the set of the audio files corresponding to such events using standard Windows tools **Start → Settings → Control Panel → Sounds and Audio Devices → Sounds**.
- **Use system tray icon animation** – enable the icon animation depending on the task performed by Kaspersky Anti-Virus. For example, a blinking envelope above the icon indicates that the application is scanning an e-mail message.
- **Log all reports** – enable recording of all reports, created during the program operation: information messages, error notifications, etc. By default, this mode is disabled and only important reports are logged, such as program's completion with an error, interruption of a task execution, etc.
- **Do not store reports longer than ... days** – by default, reports are kept for thirty days. This period may be changed by entering a value in the field on the right side. To remove this restriction, uncheck the corresponding box. While Kaspersky Anti-Virus is loading, a check for reports stored longer than the specified period will be performed and obsolete reports will be deleted.

The **Confirmation prompts** section allows the user to control displaying notifications about certain events in the operation of Kaspersky Anti-Virus. As a rule, all notifications are displayed for user's reference. For more details about configuring the confirmation prompts see section 14.10 on page 101).

Using the **Efficiency** tab (see Figure 49) you can configure restrictions imposed on the on-demand scan in order to save the battery charge (if you are using a notebook) and the operating system's resources (details see section 14.11 on page 102).

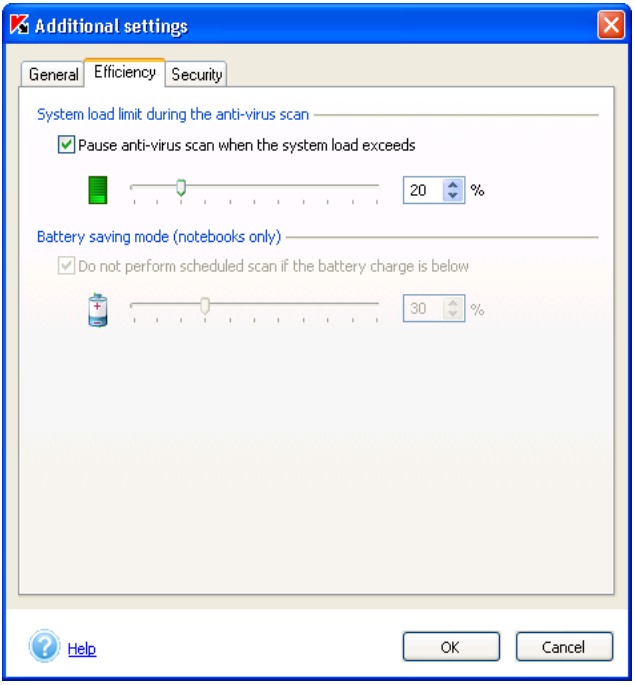

Figure 49. Additional settings of Kaspersky Anti-Virus Personal. The **Efficiency** tab

The **Security** tab (see Figure 51) contains the following settings:

- **Launch Kaspersky Anti-Virus at the system startup** – enable the automatic launch of Kaspersky Anti-Virus when the operating system is restarted.

  We strongly recommend that you do not disable the automatic launch of Kaspersky Anti-Virus because this increases the risk of your computer becoming infected.

  You cannot modify this setting if you do not have Administrator's rights for this computer.

- **Use recovery after errors system** – enable Kaspersky Anti-Virus operation recovery after a failure. If the operation of the application was interrupted, the main Kaspersky Anti-Virus window will be minimized (if it was open) and an information message will appear above the icon the in the system tray (see Figure 50). After this the application will recover automatically.

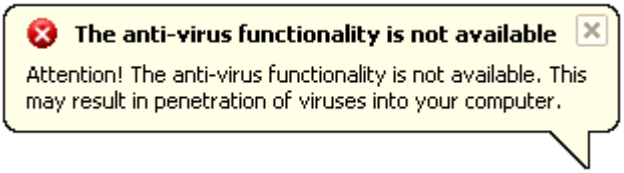
The anti-virus functionality is not available
Attention! The anti-virus functionality is not available. This may result in penetration of viruses into your computer.

Figure 50. Application failure

Use password for application protection – enable prompting for password when switching to the administrator's mode. We recommend that you use this mode if there are other users who have access to your computer whom you do not want to alter your anti-virus protection settings, disable the real-time protection or close Kaspersky Anti-Virus (details see section 14.12 on page 102). After you have enabled this option, enter the required number of characters in the **Password** field and then retype the password in the **Confirm password** field.

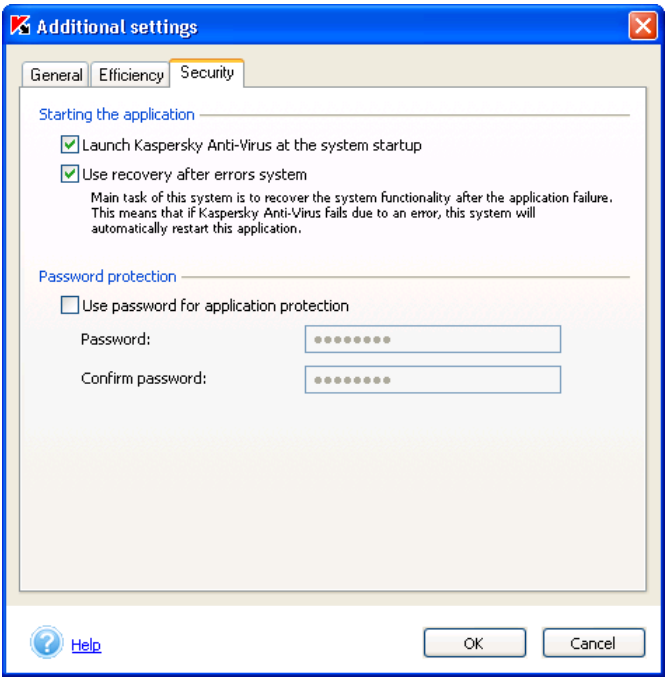
Additional settings
General
Efficiency
Security
Starting the application
Launch Kaspersky Anti-Virus at the system startup
Use recovery after errors system
Main task of this system is to recover the system functionality after the application failure. This means that if Kaspersky Anti-Virus fails due to an error, this system will automatically restart this application.
Password protection
Use password for application protection
Password:
Confirm password:
Help
OK
Cancel

Figure 51. Additional settings of Kaspersky Anti-Virus Personal. The **Security** tab.

14.10. Configuring prompts for confirmation

If you wish to be notified about certain events that happen during the program's operation, follow the Additional Settings hyperlink in the left part of the **Settings** tab (see Figure 6). Press the **Configure…** button in the **Confirmation prompts** section of the additional settings window that will open. As a result you will switch to the **Confirmation prompts settings** dialog box (see Figure 52).

The following events are provided for:

- **Prompt for the scan cancellation confirmation** – display a prompt for the user to confirm an on-demand scan cancellation. When the scan is cancelled, a tooltip message will appear above the application icon in the system tray clarifying the reasons why the scan was cancelled.

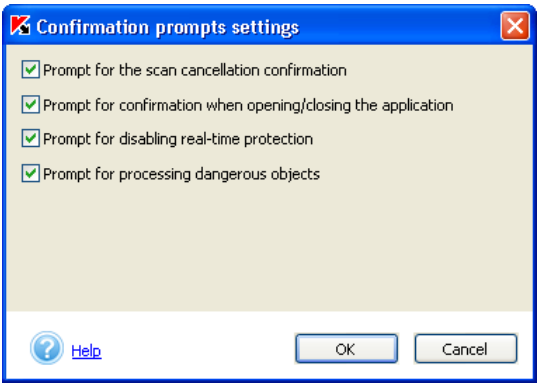

Figure 52. Configuring confirmation prompts

- **Prompt for confirmation when opening/closing the application** – display a prompt to confirm opening/closing Kaspersky Anti-Virus Personal.
- **Prompt for disabling real-time protection** – display warning messages to notify that that real-time protection of your computer was completely disabled.
- **Prompt for processing dangerous objects** – display warnings stating that some infected objects remained unprocessed after the anti-virus scan.

14.11. Restricting the functionality of Kaspersky Anti-Virus

You can impose restrictions on launching Kaspersky Anti-Virus on demand scan in cases when you need to restrict the use of your computer's resources. In order to do it, follow the Additional settings hyperlink in the left part of the **Settings** tab (see Figure 6). In the additional settings configuration dialog box that will open switch to the **Efficiency** tab (see Figure 49).

You can impose the following restrictions:

- **Pause anti-virus scan when the system load exceeds… %** - pause the on-demand anti-virus scan if the load on the file system exceeds the specified level. Once the file system load returns to the allowable level, the scan will be resumed. Specify the value for the allowable system load level using a slider or by entering this value in the field to the right of the slider (in percents) to pause the on-demand scan once this level is exceeded.

  This setting applies only to the on-demand scan tasks (for example a selected object scan task). Real-time anti-virus scan will not be interrupted.

- **Do not perform scheduled scan if the battery charge is below** – cancel the scheduled scan if you are using a portable computer and the battery charge is below a specified level. Specify the value for the allowable battery charge level using a slider or by entering this value in the field to the right of the slider (in percents) and the scheduled scan will be cancelled once the charge goes below this level.

  This option is available only if Kaspersky Anti-Virus is installed on a portable computer powered from a battery.

14.12. Working in the administrator and the user mode

Kaspersky Anti-Virus can operate in two modes: the administrator and the user mode. The use of these modes can be useful if there is another user who has access to your computer. You can prohibit to this user to modify the anti-virus protection settings, disable the real-time protection and close Kaspersky Anti-Virus. In the user mode, the application interface changes, unavailable settings are no displayed (for example the main application window does not contain the **Settings** tab).

In order to enable the use of the user and the administrator mode:

Check the **Use password for application protection** box in the **Security** tab (see Figure 51) in the Kaspersky Anti-Virus **Additional settings** dialog box. Enter the required password in the **Password** field and retype it in the **Confirm password** field.

As the result, command **Switch to the user mode** will appear in the application shortcut menu (see Figure 4) that you can use to switch to the user mode. In order to return to the administrator mode, use the **Switch to the administrator mode** command and enter the password in the window that will open (see Figure 53).

If the **Use password for application protection** box (see Figure 51) is not checked, Kaspersky Anti-Virus starts and operates in the administrator mode.

Figure 53. Entering the password

14.13. Managing Kaspersky Anti-Virus configuration

Kaspersky Anti-Virus allows the user to create and use various configurations in its operation. Now you can configure a certain mode of the programs' operation, save its settings in a special configuration file (profile) and use this configuration when it is needed.

In order to access the program configuration tools, follow the **Managing profiles** hyperlink in the left part of the **Settings** tab (see Figure 6).

You can save the current application settings in a special configuration file by pressing the **Save profile…** button or apply the settings of any configuration created earlier by pressing the **Load profile...** button. Since some modes of operation can be activated only when the operating system is started, a system restart may be required when you load some settings.

In order to restore the recommended settings, press the **Restore profile** button.

CHAPTER 15. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup and operation of the Kaspersky Anti-Virus; here we shall try to answer them here in detail.

Question: Is it possible to use Kaspersky Anti-Virus with anti-virus products of other vendors?

No. We recommend uninstalling anti-virus products of other vendors prior to installation of Kaspersky Anti-Virus to avoid software conflicts.

Question: Kaspersky Anti-Virus does not rescan files that have been scanned earlier. Why?

This is true. Kaspersky Anti-Virus does not rescan files that have not changed since the last scan.

That has become possible due to new iChecker and iStreams technologies. The technology is implemented in the program using a database of file checksums and file checksum storage in alternate NTFS streams.

Question: Why does Kaspersky Anti-Virus cause a certain decrease in server performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the anti-virus software, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases. In contrast, Kaspersky Lab believes that the purpose of its anti-virus applications is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 700 formats of archived and compressed files. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. That is achieved through the use of new, exclusive technologies, such as iChecker™ and iStreams™, developed at Kaspersky Lab.

Question: Why do I need the license key file? Will my copy of the anti-virus application work without it?

No, Kaspersky Anti-Virus does not work without a license key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work either for two weeks or for a month. When this period expires, the key will be blocked.

Question: What happens when the license expires?

After expiration of the license, Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. The anti-virus application will continue cleaning infected objects but only using the old anti-virus database.

If such a situation arises contact the company from which you purchased Kaspersky Anti-Virus or Kaspersky Lab directly for license extension.

Question: What are the regular updates for?

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by rare updates to its anti-virus database. However, recent virus epidemics spread around the world in several hours, and anti-virus protection with old database may be helpless against a new threat. In order to resist new viruses, you should update the anti-virus database on a daily basis.

Each year Kaspersky Lab increases the frequency of its issued updates to the anti-virus database. Currently it is updated every hour.

Updating of the Anti-Virus application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.

Question: What are the changes to the updating service of version 5.0?

The Kaspersky Lab 5.0 product suite features a new updating service which has been developed in accordance with the requests of our users. It automates the whole updating procedure, from the preparation of updates in Kaspersky Lab to the moment that relevant files are updated on clients' computers.

Advantages of the new updating service include:

- *Ability to resume downloading of files after disconnection*. Upon reconnection only files which have not been downloaded are retrieved.
- Cumulative updates are now half the size. A cumulative update contains the whole anti-virus database, therefore its size exceeds considerably the size of typical updates. The new service employs a special technology which allows using already existing anti-virus database for a cumulative update.
- *Accelerated downloading from the Internet*. Kaspersky Anti-Virus picks up a Kaspersky Lab's updates server located in your region. Furthermore, servers are allocated according to their performance, so you will not be sent to an overloaded server while there is another idle server available.
- *Use of key «black lists»*. Unlicensed and illegal users are now prevented from using the updating service. Licensed users therefore do not suffer from inability to contact overloaded updates' servers.
- Corporate enterprises can now create a local updates' server. This feature is designed for organizations where a single LAN unites computers protected by Kaspersky Lab products. Any computer on the LAN can be turned into an updates' server that retrieves updates from the Internet and shares them with the other networked computers.

Question: Can an intruder replace my anti-virus database?

All Kaspersky Lab anti-virus databases are supplied with a unique signature verified by Kaspersky Anti-Virus when the program is using them. If the signature supplied with the updated database does not match the signature assigned by Kaspersky Lab and if the database was released after your license for the product expired, Kaspersky Anti-Virus will not use such database.

Question: after the installation of Kaspersky Anti-Virus my connection to the local area network/internet was lost. What should I do?

This means that you a firewall is installed on your computer. This resulted in a conflict with a network attacks protection module.

1. Open main application window of Kaspersky Anti-Virus Personal and switch to the **Settings** tab (see Figure 6).
2. Using the Real-time protection link, switch to the **Real-time protection** dialog box (see Figure 17).
3. In the window that will open (see Figure 32) check the **Disable protection against network attacks** and press the **OK** button.

In order to apply settings you have configured you have to restart your computer. In order to do this press the **Yes** button. If you wish to restart your computer later, press the **No** button.

APPENDIX A. CONTACTING TECHNICAL SUPPORT

Kaspersky Lab's Technical Support is available to all registered users of Kaspersky Anti-Virus in the following cases:

- If the application seems to work improperly and errors are frequently encountered.
- If Kaspersky Anti-Virus detects a suspicious file that contains critical data and the application denies access to it, while you need to continue working with the file.

To send a message to Kaspersky Lab's Technical Support about any failures encountered during application operation:

click Send question to technical support in the left section of the **Support** tab (see Figure 7) of the main application window.

The application will automatically create a new message using the default mail client program installed in your computer, for example, Microsoft Outlook. It will automatically attach a text file to the message with a description of your system and all required data about your copy of Kaspersky Anti-Virus Personal. You should provide a detailed description of the application fault that you encountered and send the message. Our technical consultants will respond to your request as soon as possible.

If Kaspersky Anti-Virus quarantines a file that is possibly infected, you may wish to update the anti-virus databases and try to disinfect the object (for details see section 14.5, page 87). However, if this attempt to disinfect the file fails and you urgently need this file, please feel free to send the file to Kaspersky Lab for expert analysis. The file may be infected with an unknown virus or it may be a false alarm situation.

Attention! You may send files that you suspect to be infected to Kaspersky Lab only after you have scanned them using the database updated on the day you are sending the file.

To send a file to Kaspersky Lab for expert analysis:

select the file in the **Quarantine** window (see Figure 39) and click the Send button.

The application will automatically create and open a new message using the default mail client program installed in your computer, for example, Microsoft

Outlook Express, with the suspicious file attached. Send this message. Kaspersky Lab will analyze the file you have sent and try to recover all data it contains. Whatever the outcome of the recovery, you will receive a detailed report with the results of the analysis.

Note that each of the files you send must have been scanned with Kaspersky Anti-Virus maximum one day before you send it.

It may happen that even though Kaspersky Anti-Virus does not detect any possibly infected files during the scan, you feel certain that one or more files in your computer are infected with a new virus. You can send such files to Kaspersky Lab for analysis.

To send files you suspect of being infected to Kaspersky Lab for expert analysis:

click Send file for analysis in the left section of the **Support** tab (see Figure 7). Select suspicious files using a standard Windows file selection dialog box.

The subsequent steps required to send a mail message to Kaspersky Lab are identical to the procedure of sending possibly infected objects from the **Quarantine** window.

APPENDIX B. GLOSSARY

While reading this User's Guide you will encounter terms that have meanings specific to anti-virus protection. The intention of this Appendix is to provide an explanation of the meaning of such terms. The entries are listed in alphabetical order to simplify the search for the explanation you need.

A

Anti-virus database – A database created by Kaspersky Lab that contains a detailed description of all currently existing viruses and the methods used for their detection and disinfection. Our anti-virus database is regularly updated with information about new viruses as they appear; therefore, to keep your computer constantly protected from viruses, you need to *update* your anti-virus database as often as possible.

Anti-virus protection status – The current status of the anti-virus protection that characterizes the security level for your computer.

Archives – Files that include one or several files, which, in turn, can be archives.

B

Backing up – Creating a backup copy of a file in the BACKUP folder before treating it (disinfection or deleting). This file can later be restored from the backup copy, for example, for subsequent scanning with the current version of the anti-virus database.

BACKUP – A directory that contains backup copies of deleted and disinfected objects.

Boot sector – A special disk area that contains the operating system loader program.

Boot virus – A virus infecting *boot sectors* of computer disks. During a system boot, the virus forces the system to read it into memory and to surrender control from the original loader code to the viral code.

C

Computer memory – RAM installed in your computer.

D

Dangerous object – An object containing a virus. We recommend that you refrain from accessing such objects because this may lead to infection of your computer. If a dangerous object is found, we recommend that you *disinfect* it using Kaspersky Anti-Virus or delete it if disinfection is not possible.

Deleting an object – A method of treating an object. To delete an object means to remove it physically from your computer. This method is recommended for dangerous objects that for whatever reason cannot be disinfected.

Disk boot sector – An area on your hard drive or on any removable media (for example, a floppy disk or a CD-ROM). There are *boot viruses* that infect disk boot sectors. Kaspersky Anti-Virus scans boot sectors for viruses and *disinfects* them if infection is detected.

Disinfection – A method of treating infected objects. Disinfection results in partial or full removal of malicious code from the infected data, or a decision that these files cannot be disinfected. Objects are disinfected using records contained in the *anti-virus database*.

E

Email databases – Special format databases that contain email messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. These databases are scanned during a full scan of your computer. In real-time protection mode, Kaspersky Anti-Virus scans all incoming and outgoing email messages for viruses as they are being sent or received.

Exclusions – User-defined settings that exclude certain objects from the scan scope. You can customize exclusion rules for *real-time protection* and for *on-demand scans*. For instance, you can exclude archives from the scan scope during a full scan or, by using masks, specify certain file types that you do not want to scan.

F

False alarm – Situations when the application flags a clean object as infected because the code contained in this file resembles a viral code.

False positive – see *false alarm*

H

Heuristic code analyzer – A highly efficient technology that allows the application to detect unknown viruses. Objects that are suspected of being infected with either an unknown virus or a modified existing virus are identified using this technology.

High speed – A protection level that enables scanning of only *objects that may potentially become infected*. This significantly reduces scan time.

I

iChecker™ technology – a technology that allows to increase the speed of the anti-virus scan by excluding objects that have remain unchanged since the moment they had been last scanned, provided that the scan settings (the anti-virus database and settings) have not changed. The

relevant information used by the technology is stored in a special database.

For instance, you have an archived file that was scanned by Kaspersky Anti-Virus and assigned the "not infected" status. Next time this archive will be excluded from the scan scope if it has remained intact since then and the scan settings have not changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive will be re-scanned.

The use of the iChecker™ technology is restricted to scanning only those objects that have structure known to Kaspersky Anti-virus (for example, exe, dll, lnk, tiff, inf, sys, com, chm, zip, rar).

iStreams™ technology – a technology similar to **iChecker™**. The difference between the two technologies is that when the iStreams™ technology is used, the information about the object scan results is stored in an additional file stream. Besides, the iStreams™ technology can be applied when scanning objects of any type irrespective of whether or not the structure of the object is known to Kaspersky Anti-Virus.

The iStreams™ technology is restricted to the use on NTFS file system disks only.

K

Kaspersky Anti-Virus modules – Program library files included in the distributed copy of Kaspersky Anti-Virus Personal. Each of these modules corresponds to a specific function of Kaspersky Anti-Virus, such as *real-time protection, on-demand scanning, updating.*

L

License key – A file with the *.key* extension that serves as your personal "key" required for the proper operation of Kaspersky Anti-Virus Personal. The license key is included in the distribution kit if you purchase your copy of Kaspersky Anti-Virus from a Kaspersky Lab dealer. If you purchase the product online, the license key file will be sent to you via email. Kaspersky Anti-Virus WILL NOT WORK without the license key.

License period – A period during which you have the right to use Kaspersky Anti-Virus. The license period is defined by a valid license key and is, as a rule, one year from the date of purchase. After your license expires, the product will still work but you will not be able to update the *anti-virus database*.

M

Malware – the word is a contraction of “malicious software” and is a generic term for viruses, Trojans and worms.

Maximum protection – A protection level that ensures the maximum protection level that can be provided by Kaspersky Anti-Virus. With this protection mode, all files stored on your hard drive, removable media and network drives (if connected to your computer) are scanned for viruses.

O

OLE object – An object linked or embedded into another file. Kaspersky Anti-Virus scans such objects for viruses. For example, a Microsoft Excel spreadsheet embedded in a Microsoft Word document will be scanned by Kaspersky Anti-Virus as an OLE object.

On-demand scan – A mode of application operation initiated by the user that performs a scan of files of all types resident on your computer.

P

Packed files – Files containing a program and instructions for the program execution by the operating system.

Patch – A package of files used for updating programs. Patches are downloaded from the Internet and installed on your computer.

Possibly infected object – An object that contains code of an unknown virus or a code reminiscent of a known virus. Possibly infected objects are detected by the *heuristic code analyzer*.

Potentially infectable object – An object that has the potential to be infected. Potentially infectable objects are usually executable files, i.e. files with the *com*, *exe* and other extensions.

Prevention – A set of measures taken to prevent viruses from penetrating your computer. Computer virus prevention includes comprehensive anti-virus protection and retrieving current updates to your application.

Q

Quarantine – A folder to which Kaspersky Anti-Virus moves all *possibly infected objects* found during either a *full scan of your computer* or in *real-time protection* mode.

Quarantining (moving to the quarantine folder) – A method of treating an *infected* or *possibly infected object* by denying normal access to the object and moving it to the quarantine folder for subsequent treatment.

R

Real-time protection – A mode of Kaspersky Anti-Virus operation when it is launched automatically at the system startup, in which all objects are scanned for viruses when they are accessed for reading, writing, or executing. If an object is identified as *dangerous* or *suspicious*,

Kaspersky Anti-Virus will deny access to it and attempt to treat it (disinfect, quarantine, delete it, etc.) or prompt the user for action.

Recommended level – A level of anti-virus protection using settings recommended by Kaspersky Lab, which ensures the optimal protection of your computer. This level corresponds to the default settings.

Recovering, restoring – Moving an object from the *Quarantine or from the Backup storage* to its original folder, where it was located before it was quarantined/backed up, disinfected, or deleted, or to a folder specified by the user.

Report only – In this mode, when the application detects infected or suspicious objects it blocks access to them (in the real-time protection mode) and reports the detection in the task report log.

S

Scripts – A program file containing a sequence of actions which can, for example, be embedded into a web page and executed by the web browser (e.g. Microsoft Internet Explorer), or be standalone files for execution by the Windows operating system. In real-time protection mode, Kaspersky Anti-Virus monitors the execution of scripts, disables them, and scans for viruses. Depending on the results of the scan, you can, for example, allow or prohibit the script's execution. When a suspicious script is detected, its execution will be blocked.

Skip – Method of treatment in which access to the object (only in real-time protection mode) will be denied, and information about the object will be recorded in the application operation report, but no other actions on the object will be performed.

Startup objects – A set of programs required for launching and correct operation of the operating system and other programs installed on your computer. Your operating system runs these objects during each startup. Some viruses infect startup objects and can prevent the operating system from loading.

Suspicious object – see *possibly infected object*.

U

Unknown virus – A new virus that is not registered in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using the *heuristic code analyzer* and objects containing these viruses are flagged as *possibly infected*.

Updating the anti-virus database – A function of Kaspersky Anti-Virus that maintains the validity of the anti-virus protection of your computer. The updating process includes copying the *anti-virus database* from the Kaspersky Lab *update servers* to your computer and automatic integration of the database with Kaspersky Anti-Virus Personal.

Update servers – A list of http- and ftp-servers updated regularly by Kaspersky Lab from which Kaspersky Anti-Virus copies the most recent version of the anti-virus database to your computer.

V

Virus attack – A series of purposeful attempts to infect a computer with a virus.

APPENDIX C. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

C.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP as well as MS Office applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A unique second-generation heuristic analyzer efficiently detects unknown viruses. A simple and convenient interface allows users to configure the program quickly making work with it easier than ever.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks.
- **Real-time automatic protection** of all accessed files from viruses.
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases.
- **Behavior blocker** that provides maximum protection of MS Office applications against viruses.
- **Archive scanning –** Kaspersky Anti-Virus recognizes over 900 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** and **ICE** archives.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, Kaspersky® Anti-Hacker blocks the suspicious application from accessing the network. This helps ensure enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite is a software suite designed for organizing comprehensive protection of personal computers running Microsoft Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection of data saved on your computer
- protection against spam for users of Microsoft Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current status of virus activity and fresh news. The program reads the list of available news channels and their content from news server of Kaspersky Lab with specified frequency.

The product performs the following functions:

- It visualizes in the system tray the current status of virus activity.
- The product allows the users to subscribe and unsubscribe from news channels.
- It retrieves news from each subscribed channel with the specified frequency and notifies about fresh news.
- It allows reviewing news on the subscribed channels.
- It allows reviewing the list of channels and their status.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Windows application, which can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® On-Line Scanner

The program is a free service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus check of your computer. Kaspersky On-Line Scanner runs within your web browser using Microsoft ActiveX® technology. Thus, users can quickly test their computers in case of a slightest suspicion of malicious infection. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of hand-held computers and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both in internal memory of PDA and smartphones or on memory cards of any type) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a unique configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection[8] for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers.
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.

[8] Depending on the type of distribution kit.

- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a unique tool for automated deployment and administration.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS, and also smartphones running Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration,

including RBL lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for anti-virus processing of e-mail transmitted via SMTP. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a number of tools reducing the load on the mail system and preventing hacker attacks. DNS Black List support provides protection against e-mails coming from servers entered in these lists as sources distributing unwanted e-mail (spam).

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing mail messages as well as messages stored at the server, including letters in public folders and filters out unsolicited correspondence using "smart" spam recognition techniques in combination with Microsoft technologies. The application scans all messages arriving at an Exchange Server via SMTP protocol checking them for the presence of viruses using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes. It filters out spam based on formal attributes (mail address, IP address, letter size, heading) and analyzes the content of messages and of their attachments using "smart' technologies, including unique graphic signatures for identifying graphic SPAM. The application scans both the message body and the attached files.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html E-mail: support@kaspersky.com
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com

APPENDIX D. LICENSE AGREEMENT

End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) PURCHASED ON LINE FROM THE KASPERSKY LAB INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF 7 WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE

PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/ about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You

may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on ww.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).